Assurance Activity Report for
SpaceX Regulus

SpaceX Regulus Security Target Version 1.2

collaborative Protection Profile for Network Devices
Version 2.2e

PP-Module for Virtual Private Network (VPN) Gateways Version 1.1

AAR Version 1.1 August 2023

Evaluated by:

2400 Research Blvd, Suite 395
Rockville, MD 20850

Prepared for:

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
Space Exploration Technologies Corp

The Author of the Security Target:
Acumen Security, LLC

The TOE Evaluation was Sponsored by:
Space Exploration Technologies Corp

Evaluation Personnel:
Shaunak Shah
Brandon Solberg
Acumen Security, LLC

Common Criteria Version
Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version
CEM Version 3.1 Revision 5

Revision History

VERSION	DATE	CHANGES
0.1	2023-06-01	Initial Release
1.0	2023-06-15	First Submission
1.1	2023-08-02	Response to ECR Comments

Contents

1 TOE Overview

The SpaceX Regulus TOE is classified as a VPN Gateway, which is a Network Device composed of both hardware and software that is connected to networks and provides IPsec protection of network traffic. The SpaceX Regulus TOE is comprised of the Apogee-100 hardware running firmware version 1.0.

1.1 TOE Description

This section provides an overview of the TOE architecture, including physical boundaries, security functions, and relevant TOE documentation and references. Below is a diagram of the representative TOE deployment in its evaluated configuration:

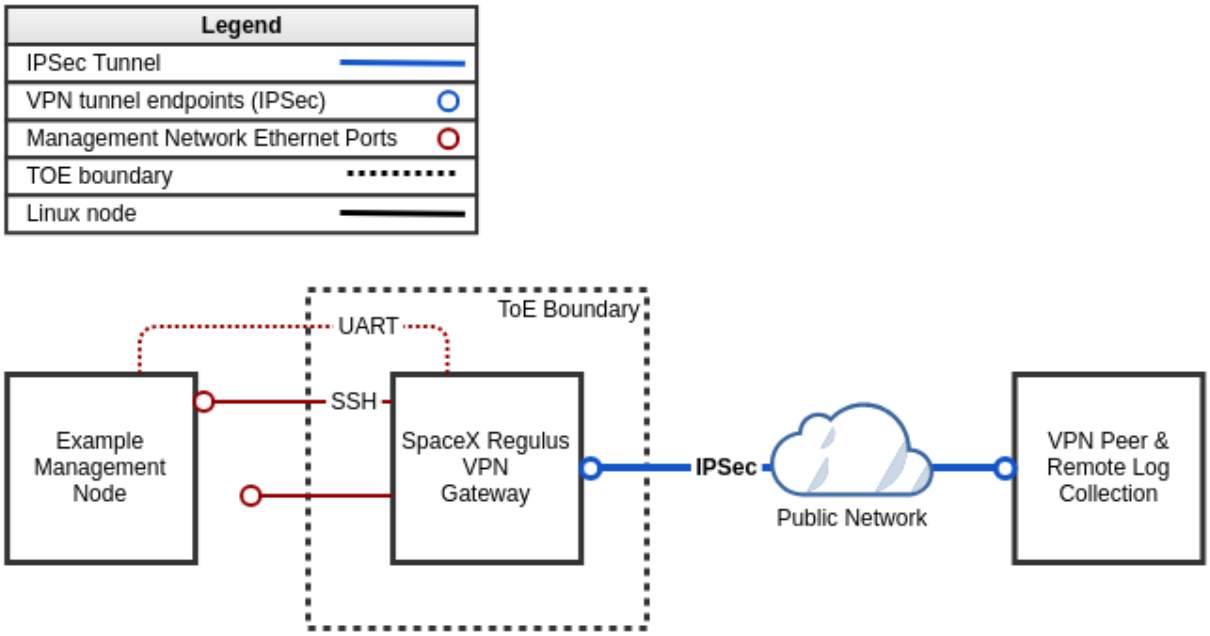


Figure 1 – Representative TOE Deployment

1.1.1 Physical Boundaries

The physical boundary of the TOE is the SpaceX Regulus chassis, which is a networked device providing connectivity to external networked entities. The TOE includes a specialized PCB board containing a Zynq Ultrascale+ ZU5 System on Chip (SoC) processor, based on Armv8-A Architecture, which executes the TOE software along with a NXP SE050F cryptographic accelerator. The TOE provides the following interfaces for management and network connectivity:

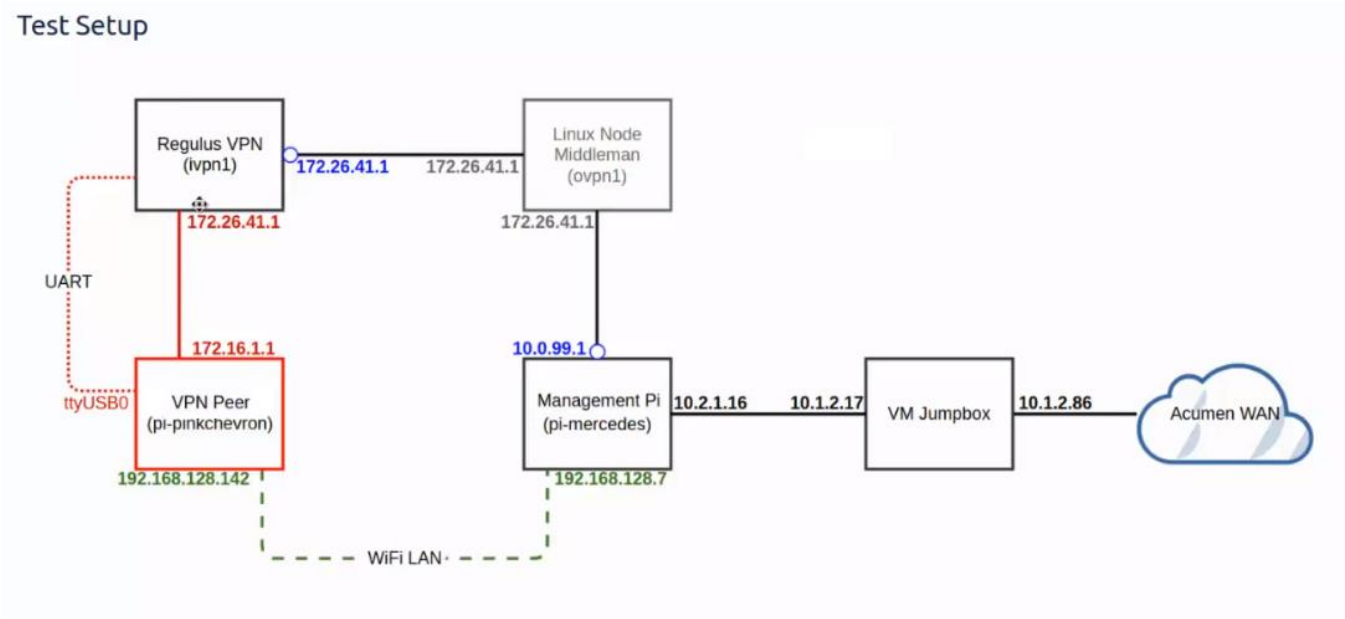
- 1x 100Mbps and 1x 10Gbps Ethernet ports for connectivity to trusted networks
- 1x 100Mbps, 1x 1Gbps, and 1x 10Gbps Ethernet ports for connectivity to untrusted networks
- UART for local serial console access
- 120VAC power input

2 Assurance Activities Identification

The Assurance Activities contained within this document include all those defined within the NDcPP 2.2e and MOD_VPNGWv1.1 based upon the core SFRs and those implemented based on selections within the PPs/EPs.

3 Test Bed Descriptions

3.1 Test Bed



3.2 Test Bed Details

Name	OS	Version	Function	Protocols	Time	Tools (version)
Tester VM (Jumpbox)	22.04 LTS	22.04 LTS	Provide access to pi's	SSH	Manually set and verified	N/A
Pi-pinkchevron	Raspbian GNU/Linux 9 (stretch)	Raspbian GNU/Linux 9 (stretch)	VPN Peer to TOE.	SSH	Manually set and verified	Syslogd Python 3.7.4 Socketserver v0.4 strongswan
Pi-mercedes	Raspbian GNU/Linux 11 (bullseye)	Raspbian GNU/Linux 11 (bullseye)	Allows management access to the TOE.	SSH	Manually set and verified	strongswan
Switch	N/A	N/A	Offer communication between the test VM and the pi's	N/A	N/A	N/A
Regulus VPN (ivpn1)	Linux-based Operating System based on Kernel 5.15	2021.02-1583-g2e001f3	TOE	SSH	Manually set and verified	N/A

3.3 Test Time & Location

All testing was carried out at the Acumen Security offices located in 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from December 2022 to June 2023.

The TOE was in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each day, the test bed was verified to ensure that it was not compromised. All evaluation documentation was always kept in a secure repository.

4 Detailed Test Cases (TSS and Guidance Activities)

4.1 TSS and Guidance Activities (Auditing)

4.1.1 FAU_GEN.1

4.1.1.1 FAU_GEN.1 TSS 1

Objective	For the administrative task of generating/import of, changing, or deleting of cryptographic keys as defined in FAU_GEN.1.1c, the TSS shall identify what information is logged to identify the relevant key.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to determine the verdict of this assurance activity. The TSS states that the TOE will audit the administrator or user whose key was changed, or the certificate to which the key belongs Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.1.1.2 FAU_GEN.1 TSS 3 (VPNGWMod)

Objective	The evaluator shall verify that the TSS describes how the TSF can be configured to log network traffic associated with applicable rules. Note that this activity may be addressed in conjunction with the TSS Evaluation Activities for FPF_RUL_EXT.1.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes how the TSF can be configured to log network traffic associated with applicable rules. Upon investigation, the evaluator found that the TSS describes how all firewall rules configured with the “Log” option cause the TOE to record the activity of that firewall rule in the audit trail. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.1.1.3 FAU_GEN.1 TSS 4 (VPNGWMod)

Objective	The evaluator shall verify that the TSS describes how the TOE behaves when one of its interfaces is overwhelmed by network traffic. It is acceptable for the TOE to drop packets that it cannot process, but under no circumstances is the TOE allowed to pass packets that do not satisfy a rule that allows the permit operation or belong to an allowed established session. It may not always be possible for the TOE to audit dropped packets due to implementation limitations. These limitations and circumstances in which the event of dropped packets is not audited shall be described in the TSS.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes how the TOE behaves when one of its interfaces is overwhelmed by network traffic. Upon investigation, the evaluator found that the TSS describes how the TOE prevents network packets from being passed without a permit rule in effect, and describes what occurs when the TOE is overwhelmed by network traffic. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.1.1.4 FAU_GEN.1 TSS 5 (VPNGWMod)

Objective	The evaluator shall also verify that the TSS describes the auditable events for IPsec peer session establishment that are required by the PP-Module.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes the auditable events for IPsec peer session establishment that are required by the PP-Module. Upon investigation, the evaluator found that the TSS describes the audit events which are logged, including the requirements of IPsec peer session establishment required by the PP-Module Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.1.1.5 FAU_GEN.1 Guidance 1

Objective	The evaluator shall check the guidance documentation and ensure that it provides an example of each auditable event required by FAU_GEN.1 (i.e. at least one instance of each auditable event, comprising the mandatory, optional and selection-based SFR sections as applicable, shall be provided from the actual audit record).
Evaluator Findings	The evaluator examined the section titled “Audit Data” in the AGD to verify that it provides an example of each auditable event required by FAU_GEN.1. Upon investigation, the evaluator found that the AGD lists all audit event records by type. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.1.1.6 FAU_GEN.1 Guidance 2

Objective	The evaluator shall also make a determination of the administrative actions related to TSF data related to configuration changes. The evaluator shall examine the guidance documentation and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the cPP. The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are related to TSF data related to configuration changes. The evaluator may perform this activity as part of the activities associated with ensuring that the corresponding guidance documentation satisfies the requirements related to it.
Evaluator Findings	The evaluator examined the AGD to verify that it identifies administrative commands, including subcommands, scripts, and configuration files, that are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the cPP. The evaluator examined the AGD and found that all necessary administrator actions are described, sufficient to enable the administrator to enforce the requirements of the cPP and PP-Module. Testing of the completeness and correctness of the AGD was done by using the AGD instructions to configure the TOE during functional testing. **The evaluator examined the AGD, and found that all** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.1.1.7 FAU_GEN.1 Guidance 3 (VPNGWMod)

Objective	The evaluator shall verify that the operational guidance describes how to configure the TSF to result in applicable network traffic logging. Note that this activity may be addressed in conjunction with the guidance Evaluation Activities for FPF_RUL_EXT.1.
Evaluator Findings	The evaluator examined the section titled “Encrypting/Decrypting Packets”, “Dropping Packets”, and “Bypassing Packets” in the AGD to verify that it provides an example of each auditable event required by FAU_GEN.1. Upon investigation, the evaluator found that the Agd references the VPN_Filter guide, which describes how to implement packet filtering by configuring the iked.conf file with the source and destination of the packet, or by defining an arbitrary network condition with the “Accept”, “Accept_log”, "drop”, or “drop_log” actions. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.1.2 FAU_STG_EXT.1

4.1.2.1 FAU_STG_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. Upon investigation, the evaluator found that the TSS describes use of an IPsec protected channel to transfer audit data to the server. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.1.2.2 FAU_STG_EXT.1 TSS 2

Objective	The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. Upon investigation, the evaluator found that the TSS describes that the TOE stores 64 MB of audit data locally. When the storage space is full, the oldest log files are deleted to make room for new files. Audit records are protected by a restrictive CLI accessible only to authenticated administrators on the “red” network segment. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.1.2.3 FAU_STG_EXT.1 TSS 3

Objective	The evaluator shall examine the TSS to ensure it describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally. The evaluator shall examine the TSS to ensure that for distributed TOEs it

	contains a list of TOE components that store audit data locally. The evaluator shall examine the TSS to ensure that for distributed TOEs that contain components which do not store audit data locally but transmit their generated audit data to other components it contains a mapping between the transmitting and storing TOE components.
Evaluator Findings	The TOE is not distributed
Verdict	Pass

4.1.2.4 FAU_STG_EXT.1 TSS 4

Objective	The evaluator shall examine the TSS to ensure that it details the behaviour of the TOE when the storage space for audit data is full. When the option 'overwrite previous audit record' is selected this description should include an outline of the rule for overwriting audit data. If 'other actions' are chosen such as sending the new audit data to an external IT entity, then the related behaviour of the TOE shall also be detailed in the TSS.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS details the behavior of the TOE when the storage space for audit data is full. Upon investigation, the evaluator found that the TSS describes how the TOE handles full local storage, by deleting the oldest log files to make room for new files. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.1.2.5 FAU_STG_EXT.1 TSS 5

Objective	The evaluator shall examine the TSS to ensure that it details whether the transmission of audit information to an external IT entity can be done in realtime or periodically. In case the TOE does not perform transmission in realtime the evaluator needs to verify that the TSS provides details about what event stimulates the transmission to be made as well as the possible acceptable frequency for the transfer of audit data.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS details whether the transmission of audit information to an external IT entity can be done in realtime or periodically. Upon investigation, the evaluator found that the TSS describes that the TOE transmits audit data to the remote audit server automatically and in real-time. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.1.2.6 FAU_STG_EXT.1 Guidance 1

Objective	The evaluator shall also examine the guidance documentation to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.
Evaluator Findings	The evaluator examined the section titled "Protected Audit Event Storage" in the AGD to verify that it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server. Upon investigation, the evaluator found that the AGD describes how to configure the IPsect session with the remote syslog server, and how to configure the TOE to transmit the

	audit records to the remote server. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.1.2.7 FAU_STG_EXT.1 Guidance 2

Objective	The evaluator shall also examine the guidance documentation to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server.
Evaluator Findings	The evaluator examined the section titled ***"Protected Audit Event Storage"*** in the AGD to verify that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. Upon investigation, the evaluator found that the AGD describes that audit logs flow over the trusted channel to the audit server. The [ST] states that such transmission is in real-time. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.1.2.8 FAU_STG_EXT.1 Guidance 3

Objective	The evaluator shall also ensure that the guidance documentation describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behavior of the TOE for each possible configuration. The description of possible configuration options and resulting behavior shall correspond to those described in the TSS.
Evaluator Findings	The evaluator examined AGD to verify that it describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behavior of the TOE for each possible configuration. Upon investigation, the evaluator found that the AGD does not describe any configuration necessary to enforce the TSF described in the [ST] and TSS; [ST] section 5.2.1.3 only selects one behaviour, which is not configurable. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2 TSS and Guidance Activities (Cryptographic Support)

Note that Test activities in the SD that are typically addressed by referencing CAVP certs are addressed in this section and are identified as "Test/CAVP" activities.

4.2.1 FCS_CKM.1

4.2.1.1 FCS_CKM.1 TSS 1

Objective	The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.
Evaluator Findings	The evaluator examined the section titled "CAVP Algorithm Certificate Details" in the Security Target to verify that the TSS identifies the key sizes supported by the TOE. Upon investigation, the evaluator found that the TSS describes the supported key sizes for all cryptographic operations.

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.1.2 FCS_CKM.1 Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target.
Evaluator Findings	The evaluator examined the section titled “Cryptographic Key Generation” in the AGD to verify that it instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target. Upon investigation, the evaluator found that the AGD describes how to configure the TOE to use only the evaluated key generation schemes and sizes. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.1.3 FCS_CKM.1 Test/CAVP 1

Objective	The evaluator shall verify the key generation mechanisms supported by the TOE.
Evaluator Findings	CAVP Certs: #A3452, C1429 – See appendix A Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.2 FCS_CKM.1.1/IKE

4.2.2.1 FCS_CKM.1.1/IKE TSS 1

Objective	The evaluator shall check to ensure that the TSS describes how the key-pairs are generated. In order to show that the TSF implementation complies with FIPS PUB 186-4, the evaluator shall ensure that the TSS contains the following information: • The TSS shall list all sections of Appendix B to which the TOE complies. • For each applicable section listed in the TSS, for all statements that are not "shall" (that is, "shall not", "should", and "should not"), if the TOE implements such options it shall be described in the TSS. If the included functionality is indicated as "shall not" or "should not" in the standard, the TSS shall provide a rationale for why this will not adversely affect the security policy implemented by the TOE; • For each applicable section of Appendix B, any omission of functionality related to "shall" or “should” statements shall be described; Any TOE-specific extensions, processing that is not included in the Appendices, or alternative Implementations allowed by the Appendices that may impact the security requirements the TOE is to enforce shall be described.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes how the key-pairs are generated. Upon investigation, the evaluator found that the TSS describes the key-pair generation method as ECC, in accordance with FIPS PUB 186-4 appendix B.4 Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

4.2.2.2 FCS_CKM.1.1/IKE Guidance 1

Objective	The evaluator shall check that the operational guidance describes how the key generation functionality is invoked, and describes the inputs and outputs associated with the process for each signature scheme supported. The evaluator shall also check that guidance is provided regarding the format and location of the output of the key generation process.
Evaluator Findings	The evaluator examined the section titled "Cryptographic Key Generation" in the AGD to verify that it describes how the key generation functionality is invoked, and describes the inputs and outputs associated with the process for each signature scheme supported. Upon investigation, the evaluator found that the AGD fully describes the process by which keys are generated, the location in the underlying file system where the keys are stored, and the format of those keys. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.2.3 FCS_CKM.1/IKE Test/CAVP 1

Objective	The evaluator shall verify the key generation mechanisms supported by the TOE.
Evaluator Findings	CAVP Certs: # A3452, C1429 – See appendix A Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.3 FCS_CKM.2

4.2.3.1 FCS_CKM.2 TSS 1 **[TD0580]**

Objective	The evaluator shall ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme. It is sufficient to provide the scheme, SFR, and service in the TSS.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. Upon investigation, the evaluator found that the TSS describes FFC and ECDSA key establishment, as selected in [ST] section 5.2.2.3 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.3.2 FCS_CKM.2 Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key establishment scheme(s).
Evaluator Findings	The evaluator examined the section titled "Cryptographic Key Generation" in the AGD to verify that it instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). Upon investigation, the evaluator found that the AGD describes how to configure the TOE to use the evaluated key establishment schemes. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

4.2.3.3 FCS_CKM.2 Test/CAVP 1

Objective	The evaluator shall verify the key establishment mechanisms supported by the TOE.
Evaluator Findings	CAVP Certs: #A3452, C1429 – See appendix A Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.4 FCS_CKM.4

4.2.4.1 FCS_CKM.4 TSS 1

Objective	The evaluator shall examine the TSS to ensure it lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g. factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case. For the purpose of this Evaluation Activity the relevant keys are those keys that are relied upon to support any of the SFRs in the Security Target. The evaluator confirms that the description of keys and storage locations is consistent with the functions carried out by the TOE (e.g. that all keys for the TOE-specific secure channels and protocols, or that support FPT_APW.EXT.1 and FPT_SKP_EXT.1, are accounted for2). In particular, if a TOE claims not to store plaintext keys in non-volatile memory then the evaluator checks that this is consistent with the operation of the TOE.
Evaluator Findings	The evaluator examined the section titled “Cryptographic Key Destruction” in the Security Target to verify that the TSS lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g. factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case. Upon investigation, the evaluator found that the TSS describes the purpose, storage location, and method of zeroization for all CSPs and keys. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.4.2 FCS_CKM.4 TSS 2

Objective	The evaluator shall check to ensure the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys (e.g., file system APIs, key store APIs).
Evaluator Findings	The evaluator examined the section titled Cryptographic Key Destruction in the Security Target to verify that the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys. Upon investigation, the evaluator found that the TSS describes that keys in plaintext on non-volatile memory are destroyed by being overwritten by zeroes via a custom function in the underlaying operating system of the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.4.3 FCS_CKM.4 TSS 3

Objective	Where the TSS identifies keys that are stored in a non-plaintext form, the evaluator shall check that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an encrypted form or that it is destroyed by a method included under FCS_CKM.4.
Evaluator Findings	The evaluator examined the section titled “Cryptographic Key Destruction” in the Security Target to verify that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an encrypted form or that it is destroyed by a method included under FCS_CKM.4. Upon investigation, the evaluator found that the TSS describes the use of a hashed password file to store user account passwords on the device. Such hashes are not “encrypted”, and no KEK is used. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.4.4 FCS_CKM.4 TSS 4

Objective	The evaluator shall check that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement (see further discussion in the Guidance Documentation section below). Note that reference may be made to the Guidance Documentation for description of the detail of such cases where destruction may be prevented or delayed.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement. Upon investigation, the evaluator found that the TSS does not describe any circumstances under which the TOE would fail to conform to the requirement. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.4.5 FCS_CKM.4 TSS 5

Objective	Where the ST specifies the use of “a value that does not contain any CSP” to overwrite keys, the evaluator shall examine the TSS to ensure that it describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs. Upon investigation, the evaluator found that the [ST] does not claim “a value that does not contain any CSP” Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.4.6 FCS_CKM.4 Guidance 1

Objective	A TOE may be subject to situations that could prevent or delay key destruction in some cases. The evaluator shall check that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS (and any other supporting information used). The evaluator shall check that the guidance documentation provides

	guidance on situations where key destruction may be delayed at the physical layer.
Evaluator Findings	The evaluator examined the section titled Cryptographic Key Destruction in the AGD to verify that it identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS. Upon investigation, the evaluator found that the AGD does not describe any circumstances under which the TOE would fail to conform to the requirement. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.5 FCS_COP.1/DataEncryption

4.2.5.1 FCS_COP.1/DataEncryption TSS 1

Objective	The evaluator shall examine the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the TSS describes the key sizes and modes supported by the TOE as AES with 256-bit keys in CBC or GCM modes Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.5.2 FCS_COP.1/DataEncryption Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption.
Evaluator Findings	The evaluator examined the section titled “SSH Configuration Options” and “Configuring IPsec Parameters” in the AGD to verify that it provides guidance instructs the administrator how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the AGD fully describes how to configure the TOE to implement only the evaluated modes and key sizes for encryption. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.5.3 FCS_COP.1/DataEncryption Test/CAVP 1

Objective	The evaluator shall verify the implementation of encryption supported by the TOE.
Evaluator Findings	CAVP Certs: #A3452, A3121 – See appendix A Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.6 FCS_COP.1/SigGen

4.2.6.1 FCS_COP.1/SigGen TSS 1

Objective	The evaluator shall examine the TSS to determine that it specifies the cryptographic algorithm

	and key size supported by the TOE for signature services.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS to ensure it specifies the cryptographic algorithm and key size supported by the TOE for signature services. Upon investigation, the evaluator found that the TSS describes signature services using an ECDSA key over P-256 or P-384, or an RSA key of 4096 bits. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.6.2 FCS_COP.1/SigGen Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services.
Evaluator Findings	The evaluator examined the section titled “SSH Configuration Options” and “Configuring IPsec Parameters” in the AGD to verify that it provides guidance instructs the administrator how to configure the TOE to use the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services. Upon investigation, the evaluator found that the AGD fully describes how to configure the TOE to use only the evaluated cryptographic algorithms and key sizes for signature services. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.6.3 FCS_COP.1/SigGen Test/CAVP 1

Objective	The evaluator shall verify the implementation of signature generation and verification supported by the TOE.
Evaluator Findings	CAVP ECDSA&SigVer SigGen (186-4) Certs: #A3120, C1429 – see appendix A Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.7 FCS_COP.1/Hash

4.2.7.1 FCS_COP.1/Hash TSS 1

Objective	The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS documents the association of the hash function with other TSF cryptographic functions. Upon investigation, the evaluator found that the TSS describes the hash functions used byIKE and SSH as SHA-384 and HMAC-SHA-384, with SHA-256 and SHA-384 used for ECDSA signature services. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.7.2 FCS_COP.1/Hash Guidance 1

Objective	The evaluator shall check the AGD documents to determine that any configuration that is required to configure the required hash sizes is present.

Evaluator Findings	The evaluator examined the section titled “SSH Configuration Options” and “Configuring IPsec Parameters” in the AGD to verify that it presents any configuration that is required to configure the required hash sizes. Upon investigation, the evaluator found that the AGD fully describes how to configure the TOE to use only the approved hash algorithms. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.7.3 FCS_COP.1/Hash Test/CAVP 1

Objective	The evaluator shall verify the implementation of hashing supported by the TOE.
Evaluator Findings	CAVP Certs: #A3452, A3122 – See appendix A Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.8 FCS_COP.1/KeyedHash

4.2.8.1 FCS_COP.1/KeyedHash TSS 1

Objective	The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used. Upon investigation, the evaluator found that the TSS describes the HMAC function for IPsec as HMAC-SHA-384 with key length of 256 bits, block size of 128 bits, and output MAC length of 48 bytes. For SSH, the TOE implements HMAC-SHA-384 with 256-bit keys, block size 128 bits, and output MAC of 64 or 32 bytes. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.8.2 FCS_COP.1/KeyedHash Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function.
Evaluator Findings	The evaluator examined the section titled “SSH Configuration Options” and “Configuring IPsec Parameters”in the AGD to verify how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function. Upon investigation, the evaluator found that the AGD fully describes how to configure the TOE to use only the evaluated hash functions. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.8.3 FCS_COP.1/KeyedHash Test/CAVP 1

Objective	The evaluator shall verify the implementation of MACing supported by the TOE.

Evaluator Findings	CAVP Certs: #A3452, A3121 – see appendix A Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.9 FCS_RBG_EXT.1

4.2.9.1 FCS_RBG_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min-entropy contained in the combined seed value.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min-entropy contained in the combined seed value. Upon investigation, the evaluator found that the TSS describes the entropy source as a platform based hardware noise source, and the DRBG as counter-DRBG with AES 256. The TOE seeds the DRBG with a minimum of 256 bits of data. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.9.2 FCS_RBG_EXT.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains appropriate instructions for configuring the RNG functionality.
Evaluator Findings	The evaluator examined the section titled “Cryptographic Operation (Random Bit Generation)” in the AGD to verify that it contains appropriate instructions for configuring the RNG functionality. Upon investigation, the evaluator found that the AGD states that no configuration is necessary or possible. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.2.9.3 FCS_RBG_EXT.1.1 Test/CAVP 1

Objective	The evaluator shall verify the implementation of SP 800-90A DRBG supported by the TOE.
Evaluator Findings	CAVP Certs: # C886 – see appendix A Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3 TSS and Guidance Activities (IPsec)

4.3.1 FCS_IPSEC_EXT.1

4.3.1.1 FCS_IPSEC_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS and determine that it describes what takes place when a packet is processed by the TOE, e.g., the algorithm used to process the packet. The TSS describes how the SPD is implemented and the rules for processing both inbound and outbound packets in terms of the IPsec policy. The TSS describes the rules that are available and the

	resulting actions available after matching a rule. The TSS describes how those rules and actions form the SPD in terms of the BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet), and PROTECT (e.g., encrypt the packet) actions defined in RFC 4301.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes what takes place when a packet is processed by the TOE. Upon investigation, the evaluator found that the TSS describes the operation of the IPsec system, including the SDP and the rules for BYAPSS, DISCARD, or PROTECT operations. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.2 FCS_IPSEC_EXT.1.1 TSS 2

Objective	As noted in section 4.4.1 of RFC 4301, the processing of entries in the SPD is non-trivial and the evaluator shall determine that the description in the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges, conditional rules, etc., the evaluator shall determine that the description of rule processing (for both inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the case where two different rules may apply. This description shall cover both the initial packets (that is, no SA is established on the interface or for that particular packet) as well as packets that are part of an established SA.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. Upon investigation, the evaluator found that the TSS describes the exact operation of the SPD and the IPsec system, including the order of rule processing operations. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.3 FCS_IPSEC_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to construct entries into the SPD that specify a rule for processing a packet. The description includes all three cases – a rule that ensures packets are encrypted/decrypted, dropped, and flow through the TOE without being encrypted. The evaluator shall determine that the description in the guidance documentation is consistent with the description in the TSS, and that the level of detail in the guidance documentation is sufficient to allow the administrator to set up the SPD in an unambiguous fashion. This includes a discussion of how ordering of rules impacts the processing of an IP packet.
Evaluator Findings	The evaluator examined the section titled “Encrypting/Decrypting Packets”, “Dropping Packets”, and “Bypassing Packets” in the AGD to verify that it instructs the Administrator how to construct entries into the SPD that specify a rule for processing a packet. Upon investigation, the evaluator found that the AGD references the VPN_Filter guide, which describes the exact steps needed to configure the TOEs SDP and its operation. The evaluator verified that the level of detail in AGD is sufficient to allow the administrator to set up the SPD unambiguously. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.4 FCS_IPSEC_EXT.1.3 TSS 1

Objective	The evaluator checks the TSS to ensure it states that the VPN can be established to operate in transport mode and/or tunnel mode (as identified in FCS_IPSEC_EXT.1.3).
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS states that the VPN can be established to operate in transport mode and/or tunnel mode (as identified in FCS_IPSEC_EXT.1.3). Upon investigation, the evaluator found that the TSS states that the TOE only operates in tunnel mode. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.5 FCS_IPSEC_EXT.1.3 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions on how to configure the connection in each mode selected.
Evaluator Findings	The evaluator examined the section titled IKE Mode in the AGD to verify that it contains instructions on how to configure the connection in each mode selected. Upon investigation, the evaluator found that the AGD states that the TOE only functions in tunnel mode. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.6 FCS_IPSEC_EXT.1.4 TSS 1

Objective	The evaluator shall examine the TSS to verify that the selected algorithms are implemented. In addition, the evaluator ensures that the SHA-based HMAC algorithm conforms to the algorithms specified in FCS_COP.1/KeyedHash Cryptographic Operations (for keyed-hash message authentication) and if the SHA-based HMAC function truncated output is utilized it must also be described.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS states that the selected algorithms are implemented. Upon investigation, the evaluator found that the TSS lists the supported IPsec algorithms, which conform to the selections in [ST] section 5.2.2.9 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.7 FCS_IPSEC_EXT.1.4 Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure it provides instructions on how to configure the TOE to use the algorithms selected.
Evaluator Findings	The evaluator examined the section titled IKE Algorithms in the AGD to verify that it provides instructions on how to configure the TOE to use the algorithms selected. Upon investigation, the evaluator found that the AGD describes the only supported algorithms for IPsec, and how to configure the TOE to implement these algorithms. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.8 FCS_IPSEC_EXT.1.5 TSS 1

Objective	The evaluator shall examine the TSS to verify that IKEv1 and/or IKEv2 are implemented.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS identifies whether IKEv1 and/or IKEv2 are implemented. Upon investigation, the evaluator found that the TSS states that the TOE implements only IKEv2 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.9 FCS_IPSEC_EXT.1.5 TSS 2

Objective	For IKEv1 implementations, the evaluator shall examine the TSS to ensure that, in the description of the IPsec protocol, it states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used. It may be that this is a configurable option.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used. Upon investigation, the evaluator found that the TSS describes only the use of IKEv2 mode, in main mode only. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.10 FCS_IPSEC_EXT.1.5. Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure it instructs the administrator how to configure the TOE to use IKEv1 and/or IKEv2 (as selected), and how to configure the TOE to perform NAT traversal (if selected).
Evaluator Findings	The evaluator examined the section titled IKE Mode in the AGD to verify that it instructs the administrator how to configure the TOE to use IKEv1 and/or IKEv2 (as selected), and how to configure the TOE to perform NAT traversal (if selected). Upon investigation, the evaluator found that the AGD states that the TOE only operates in IKEv2 mode. [ST] section 5.2.2.9 does not select NAT traversal. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.11 FCS_IPSEC_EXT.1.5. Guidance 2

Objective	If the IKEv1 Phase 1 mode requires configuration of the TOE prior to its operation, the evaluator shall check the guidance documentation to ensure that instructions for this configuration are contained within that guidance.
Evaluator Findings	The evaluator examined the section titled IKE Mode in the AGD to verify that it contains any necessary instructions for IKEv1 Phase 1 mode configuration. Upon investigation, the evaluator found that the AGD states that the TOE only operates in IKEv2 mode. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.12 FCS_IPSEC_EXT.1.6 TSS 1

Objective	The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms chosen in the selection of the requirement are included in the TSS discussion.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms chosen in the selection of the requirement are included in the TSS discussion. Upon investigation, the evaluator found that the TSS describes the encryption algorithms for IPsec as AES-CBC-256. Based on these findings, this assurance activity is considered satisfied.
Verdict	pass

4.3.1.13 FCS_IPSEC_EXT.1.6 Guidance 1

Objective	The evaluator shall ensure that the guidance documentation describes the configuration of all selected algorithms in the requirement.
Evaluator Findings	The evaluator examined the section titled IKE Algorithms in the AGD to verify that it describes the configuration of all selected algorithms in the requirement. Upon investigation, the evaluator found that the AGD states that the TOE only supports AES-CBC-256, and no other algorithms for encryption. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.14 FCS_IPSEC_EXT.1.7 TSS 1

Objective	The evaluator shall ensure the TSS identifies the lifetime configuration method used for limiting the IKEv1 Phase 1 SA lifetime and/or the IKEv2 SA lifetime. The evaluator shall verify that the selection made here corresponds to the selection in FCS_IPSEC_EXT.1.5.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS identifies the lifetime configuration method used for limiting the IKEv1 Phase 1 SA lifetime and/or the IKEv2 SA lifetime and that information corresponds to the selection in FCS_IPSEC_EXT.1.5. Upon investigation, the evaluator found that the TSS describes the IKEv2 SA lifetime, which conforms to the selections in [ST] section 5.2.2.9 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.15 FCS_IPSEC_EXT.1.7 Guidance 1 **[TD0633]**

Objective	The evaluator shall verify that the values for SA lifetimes can be configured and that the instructions for doing so are located in the Guidance documentation. If time-based limits are supported, configuring the limit may lead to a rekey no later than the specified limit. For some implementations, it may be necessary, though, to configure the TOE with a lower time value to ensure a rekey is performed before the maximum SA lifetime of 24 hours is exceeded (e.g. configure a time value of 23h 45min to ensure the actual rekey is performed no later than 24h). The evaluator shall verify that the Guidance documentation allows the Administrator to configure the Phase 1 SA value of 24 hours or provides sufficient instruction about the time value to configure to ensure the rekey is performed no later than the maximum SA lifetime of

	24 hours. It is not permitted to configure a value of 24 hours if that leads to an actual rekey after more than 24hours. Currently there are no values mandated for the number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.
Evaluator Findings	The evaluator examined the section titled IKE Lifetimes in the AGD to verify that it includes instructions for configuring values for SA lifetimes. Upon investigation, the evaluator found that the AGD describes how to configure the lifetime of between 5 minutes and 24 hours for phase 1, 5 minutes to 8 hours for phase 2, or number of bytes for phase 2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.16 FCS_IPSEC_EXT.1.8 TSS 1

Objective	The evaluator shall ensure the TSS identifies the lifetime configuration method used for limiting the IKEv1 Phase 2 SA lifetime and/or the IKEv2 Child SA lifetime. The evaluator shall verify that the selection made here corresponds to the selection in FCS_IPSEC_EXT.1.5.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS identifies the lifetime configuration method used for limiting the IKEv1 Phase 2 SA lifetime and/or the IKEv2 Child SA lifetime and that the information corresponds to the selection in FCS_IPSEC_EXT.1.5. Upon investigation, the evaluator found that the TSS describes the IKev2 child Sa lifetime as bytes or minutes, which conforms to the selections in [ST] section 5.2.2.9 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.17 FCS_IPSEC_EXT.1.8 Guidance 1 **[TD0633]**

Objective	The evaluator shall verify that the values for SA lifetimes can be configured and that the instructions for doing so are located in the Guidance documentation. If time-based limits are supported, configuring the limit may lead to a rekey no later than the specified limit. For some implementations, it may be necessary, though, to configure the TOE with a lower time value to ensure a rekey is performed before the maximum SA lifetime of 8 hours is exceeded (e.g. configure a time value of 7h 45min to ensure the actual rekey is performed no later than 8h). The evaluator shall verify that the Guidance documentation allows the Administrator to configure the Phase 2 SA value of 8 hours or provides sufficient instruction about the time value to configure to ensure the rekey is performed no later than the maximum SA lifetime of 8 hours. It is not permitted to configure a value of 8 hours if that leads to an actual rekey after more than 8hours. Currently there are no values mandated for the number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.
Evaluator Findings	The evaluator examined the section titled IKE Lifetimes in the AGD to verify that it includes instructions for configuring values for SA lifetimes. Upon investigation, the evaluator found that the AGD describes how IKEv2 Phase 1 and Phase 2 SA lifetimes are set, in minutes or bytes (Phase 2 only). When configuring a minute lifetime, the phase 2 SA lifetime cannot be longer than 8 hours. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.18 FCS_IPSEC_EXT.1.9 TSS 1

Objective	The evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating "x". The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of "x" meets the stipulations in the requirement.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes the process for generating "x" for each DH group supported. Upon investigation, the evaluator found that the TSS describes how “x” is generated using the DRBG and negotiated DH group. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.19 FCS_IPSEC_EXT.1.10 TSS 1

Objective	If the first selection is chosen, the evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of the nonces meet the stipulations in the requirement. If the second selection is chosen, the evaluator shall check to ensure that, for each PRF hash supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of the nonces meet the stipulations in the requirement.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes the process for generating each nonce for each DH group or PRF hash supported and indicates that the random number generated that meets the requirements in this PP is used, and indicates that the length of the nonces meet the stipulations in the requirement. Upon investigation, the evaluator found that the TSS describes the process for creating nonces by using the DRBG and the negotiated DH group. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.20 FCS_IPSEC_EXT.1.11 TSS 1

Objective	The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS lists the DH groups specified in the requirement as being supported. Upon investigation, the evaluator found that the TSS lists the supported DH groups, which conform to the selections made in [ST] section 5.2.2.9. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.21 FCS_IPSEC_EXT.1.11 Guidance 1

Objective	The evaluator shall ensure that the guidance documentation describes the configuration of all

	algorithms selected in the requirement.
Evaluator Findings	The evaluator examined the section titled IKE Algorithms in the AGD to verify that it describes the configuration of all algorithms selected in the requirement. Upon investigation, the evaluator found that the AGD describes all cryptographic operations which are supported by the TOE, and describes how to configure the TOE to use each algorithm. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.22 FCS_IPSEC_EXT.1.12 TSS 1

Objective	The evaluator shall check that the TSS describes the potential strengths (in terms of the number of bits in the symmetric key) of the algorithms that are allowed for the IKE and ESP exchanges. The TSS shall also describe the checks that are done when negotiating IKEv1 Phase 2 and/or IKEv2 CHILD_SA suites to ensure that the strength (in terms of the number of bits of key in the symmetric algorithm) of the negotiated algorithm is less than or equal to that of the IKE SA this is protecting the negotiation.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes the potential strengths of the algorithms that are allowed for the IKE and ESP exchanges and the checks that are done when negotiating IKEv1 Phase 2 and/or IKEv2 CHILD_SA suites. Upon investigation, the evaluator found that the TSS describes the strength of the keys as 256 bits, for both phase 1 and phase 2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.23 FCS_IPSEC_EXT.1.13 TSS 1

Objective	The evaluator shall ensure that the TSS identifies RSA and/or ECDSA as being used to perform peer authentication. The description must be consistent with the algorithms as specified in FCS_COP.1/SigGen Cryptographic Operations (for cryptographic signature).
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS identifies RSA and/or ECDSA as being used to perform peer authentication and that the algorithms are consistent with those specified in FCS_COP.1/SigGen Cryptographic Operations. Upon investigation, the evaluator found that the TSS describes the use of ECDSA keys for peer authentication, which is consistent with [ST] section 5.2.2.2 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.24 FCS_IPSEC_EXT.1.13 TSS 2

Objective	If pre-shared keys are chosen in the selection, the evaluator shall check to ensure that the TSS describes how pre-shared keys are established and used in authentication of IPsec connections. The description in the TSS shall also indicate how pre-shared key establishment is accomplished for TOEs that can generate a pre-shared key as well as TOEs that simply use a pre-shared key.
Evaluator Findings	The TOE does not support PreShared Keys
Verdict	Pass

4.3.1.25 FCS_IPSEC_EXT.1.13 Guidance 1

Objective	The evaluator shall ensure the guidance documentation describes how to set up the TOE to use certificates with RSA and/or ECDSA signatures and public keys.
Evaluator Findings	The evaluator examined the section titled X509 Certificate Validation in the AGD to verify that it describes how to set up the TOE to use certificates with RSA and/or ECDSA signatures and public keys. Upon investigation, the evaluator found that the AGD fully describes the process for generating and using X.509v3 certificates with the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.26 FCS_IPSEC_EXT.1.13 Guidance 2

Objective	The evaluator shall check that the guidance documentation describes how preshared keys are to be generated and established. The description in the guidance documentation shall also indicate how pre-shared key establishment is accomplished for TOEs that can generate a pre-shared key as well as TOEs that simply use a pre-shared key.
Evaluator Findings	The TOE does not support preshared keys.
Verdict	Pass

4.3.1.27 FCS_IPSEC_EXT.1.13 Guidance 3

Objective	The evaluator will ensure that the guidance documentation describes how to configure the TOE to connect to a trusted CA and ensure a valid certificate for that CA is loaded into the TOE and marked “trusted”.
Evaluator Findings	The evaluator examined the section titled X509 Certificate Validation in the AGD to verify that it describes how to configure the TOE to connect to a trusted CA and ensure a valid certificate for that CA is loaded into the TOE and marked “trusted”. Upon investigation, the evaluator found that the AGD describes the process for importing certificates – including CA certificates. AGD describes the validation check which takes place before a certificate is “trusted” Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.28 FCS_IPSEC_EXT.1.14 TSS 1

Objective	The evaluator shall ensure that the TSS describes how the TOE compares the peer’s presented identifier to the reference identifier. This description shall include which field(s) of the certificate are used as the presented identifier (DN, Common Name, or SAN). If the TOE simultaneously supports the same identifier type in the CN and SAN, the TSS shall describe how the TOE prioritizes the comparisons (e.g. the result of comparison if CN matches but SAN does not). If the location (e.g. CN or SAN) of non-DN identifier types must explicitly be configured as part of the reference identifier, the TSS shall state this. If the ST author assigned an additional identifier type, the TSS description shall also include a description of that type and the method by which that type is compared to the peer’s presented certificate, including what field(s) are compared and which fields take precedence in the comparison.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes how the TOE compares the peer’s presented identifier to the reference identifier.

	Upon investigation, the evaluator found that the TSS describes how the TOE verifies the presented reference identifier against its reference identifier, for each type of presented identifier. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.3.1.29 FCS_IPSEC_EXT.1.14 Guidance 1

Objective	The evaluator shall ensure that the operational guidance describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not and includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s). If the identifier scheme implemented by the TOE does not guarantee unique identifiers, the evaluator shall ensure that the operational guidance provides a set of warnings and/or CA policy recommendations that would result in secure TOE use.
Evaluator Findings	The evaluator examined the section titled X509 Certificate Validation in the AGD to verify that it describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not, and includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s). Upon investigation, the evaluator found that the AGD describes the supported identifiers, and explicitly states that the TOE supports the SAN extension, and includes an explicit statement regarding which reference identifiers supersede which other. The AGD also instructions the administrator to use only fully-unique FQDNs for each peer device. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.4 TSS and Guidance Activities (SSH)

4.4.1 FCS_SSHS_EXT.1

4.4.1.1 FCS_SSHS_EXT.1.2 TSS 1 **[TD0631]**

Objective	The evaluator shall check to ensure that the TSS contains a list of supported public key algorithms that are accepted for client authentication and that this list is consistent with signature verification algorithms selected in FCS_COP.1/SigGen (e.g., accepting EC keys requires corresponding Elliptic Curve Digital Signature algorithm claims). The evaluator shall confirm that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. For example, the TOE could verify that the SSH client's presented public key matches one that is stored within the SSH server's authorized_keys file. If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, then the evaluator shall confirm its role in the authentication process is described in the TSS.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS contains a description of the public key algorithms that are acceptable for use for authentication, that this list conforms to FCS_SSHS_EXT.1.5, and that if password-based authentication methods have been selected in the ST then these are also described. Upon investigation, the evaluator found that the TSS describes the public key algorithms, which conform to the selections in [ST] section 5.2.2.11. [ST] section 5.2.2.11 does not select X.509v3 certificate-based authentication. TSS describes how the password is used in the authentication

	process over SSH. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.4.1.2 FCS_SSHS_EXT.1.3 TSS 1

Objective	The evaluator shall check that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled. Upon investigation, the evaluator found that the TSS describes large packets, and states that they will be dropped. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.4.1.3 FCS_SSHS_EXT.1.4 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS specifies the optional characteristics and the encryption algorithms supported. Upon investigation, the evaluator found that the TSS lists the cryptographic algorithms allowable by the TOE, which conform to the selections in [ST] 5.2.2.11 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.4.1.4 FCS_SSHS_EXT.1.4 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).
Evaluator Findings	The evaluator examined the section titled SSH Configuration Options in the AGD to verify that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD fully describes the method by which the TOE is configured to enforce the evaluated configuration. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.4.1.5 FCS_SSHS_EXT.1.5 TSS 1 **[TD0631]**

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the SSH server’s host public key algorithms supported are specified and that they are identical to those listed for this component.
Evaluator	The evaluator examined the section titled TSS in the Security Target to verify that the TSS

Findings	specifies the optional characteristics and the public key algorithms supported. Upon investigation, the evaluator found that the TSS lists the public key algorithms which are supported. This list is consistent with [ST] section 5.2.2.11 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.4.1.6 FCS_SSHS_EXT.1.5 TSS 2

Objective	The evaluator shall confirm that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. For example, the TOE could verify that the SSH client's presented public key matches one that is stored within the SSH server's authorized_keys file.
Evaluator Findings	The TOE does not support x.509v3 based authentication for SSH.
Verdict	Pass

4.4.1.7 FCS_SSHS_EXT.1.5 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).
Evaluator Findings	The evaluator examined the section titled SSH Configuration Options in the AGD to verify that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD fully describes how to configure the TOE to implement only the evaluated configuration. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.4.1.8 FCS_SSHS_EXT.1.6 TSS 1

Objective	The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that the list corresponds to the list in this component.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS lists the supported data integrity algorithms, and that that list corresponds to the list in this component. Upon investigation, the evaluator found that the TOE supports only GCM modes for SSH, which have an implicit data integrity algorithm. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.4.1.9 FCS_SSHS_EXT.1.6 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the "none" MAC algorithm is not allowed).
Evaluator	The evaluator examined the section titled SSH Configuration Options in the AGD to verify that it

Findings	contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE. Upon investigation, the evaluator found that the AGD does not instruct the administrator to configure the “none” MAC algorithm in the configuration of the device, which will cause that algorithm to be rejected. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.4.1.10 FCS_SSHS_EXT.1.7 TSS 1

Objective	The evaluator shall check the TSS to ensure that it lists the supported key exchange algorithms, and that the list corresponds to the list in this component.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS lists the supported key exchange algorithms, and that that list corresponds to the list in this component. Upon investigation, the evaluator found that the TSS lists the key exchange algorithms, which conform to the list in [ST] section 5.2.2.11 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.4.1.11 FCS_SSHS_EXT.1.7 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE.
Evaluator Findings	The evaluator examined the section titled SSH Configuration Options in the AGD to verify that it contains instructions to the administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE. Upon investigation, the evaluator found that the AGD describes how to configure the SSH functionality to use only the evaluated key exchange algorithms. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.4.1.12 FCS_SSHS_EXT.1.8 TSS 1

Objective	The evaluator shall check that the TSS specifies the following: a) Both thresholds are checked by the TOE. b) Rekeying is performed upon reaching the threshold that is hit first.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS specifies that both thresholds are checked and that rekeying is performed upon reaching the threshold that is hit first. Upon investigation, the evaluator found that the TSS states that rekeying is performed after no more than 512 MB or 2700 seconds, whichever comes first.. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.4.1.13 FCS_SSHS_EXT.1.8 Guidance 1

Objective	If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, then the evaluator shall check that the guidance documentation describes how to configure those

	thresholds. Either the allowed values are specified in the guidance documentation and must not exceed the limits specified in the SFR (one hour of session time, one gigabyte of transmitted traffic) or the TOE must not accept values beyond the limits specified in the SFR. The evaluator shall check that the guidance documentation describes that the TOE reacts to the first threshold reached.
Evaluator Findings	The evaluator examined the section titled SSH Configuration Options in the AGD to verify that it describes how to configure any thresholds that are conifgurable. Upon investigation, the evaluator found that the AGD describes how to configure the TOE to rekey the connection after a configurable threshold. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5 TSS and Guidance Activities (Identification and Authentication)

4.5.1 FIA_AFL.1

4.5.1.1 FIA_AFL.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked. The TSS shall also describe the method by which the remote administrator is prevented from successfully logging on to the TOE, and the actions necessary to restore this ability.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked; the method by which the remote administrator is prevented from successfully logging on to the TOE; and the actions necessary to restore this ability. Upon investigation, the evaluator found that the TSS describes the use of a counter to keep track of failed authentication events, and the locking of abusive accounts until the timer expires. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5.1.2 FIA_AFL.1 TSS 2

Objective	The evaluator shall examine the TSS to confirm that the TOE ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available, either permanently or temporarily (e.g. by providing local logon which is not subject to blocking).
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available. Upon investigation, the evaluator found that the TSS states that the TOE provides a local console, at which lockouts are not enforced and failed authentication attempts are not tracked, which can be used to administer the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5.1.3 FIA_AFL.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to ensure that instructions for configuring the number of successive unsuccessful authentication attempts and time period (if implemented) are provided, and that the process of allowing the remote administrator to once again successfully log on is described for each “action” specified (if that option is chosen). If different actions or mechanisms are implemented depending on the secure protocol employed (e.g., TLS vs. SSH), all must be described.
Evaluator Findings	The evaluator examined the section titled Authentication Failure Management in the AGD to verify that it provides instructions for configuring the number of successive unsuccessful authentication attempts and time period (if implemented), and that the process of allowing the remote administrator to once again successfully log on is described for each “action” specified (if that option is chosen). Upon investigation, the evaluator found that the AGD describes how to configure the number of successive unsuccessful authentication attempts before lockout, and the lockout period. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5.1.4 FIA_AFL.1 Guidance 2

Objective	The evaluator shall examine the guidance documentation to confirm that it describes, and identifies the importance of, any actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA_AFL.1.
Evaluator Findings	The evaluator examined the section titled Authentication Failure Management in the AGD to verify that it describes, and identifies the importance of, any actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA_AFL.1. Upon investigation, the evaluator found that the AGD states that administrators always have access to the TOE via the local interface, and lists some important factors for administrators to always maintain access to the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5.2 FIA_PMG_EXT.1

4.5.2.1 FIA_PMG_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it contains the lists of the supported special character(s) and minimum and maximum number of charters supported for administrator passwords.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS contains the lists of the supported special character(s) and minimum and maximum number of charters supported for administrator passwords. Upon investigation, the evaluator found that the TSS lists the supported special characters and password lengths. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5.2.2 FIA_PMG_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that it: a) identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords, and b) provides instructions on setting the minimum password length and describes the valid minimum password lengths supported.
Evaluator Findings	The evaluator examined the section titled Password Management in the AGD to verify that it identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords, and provides instructions on setting the minimum password length and describes the valid minimum password lengths supported. Upon investigation, the evaluator found that the AGD describes the valid minimum password lengths and the supported characters and special characters. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5.3 FIA_UIA_EXT.1

4.5.3.1 FIA_UIA_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it describes the logon process for each logon method (local, remote (HTTPS, SSH, etc.)) supported for the product. This description shall contain information pertaining to the credentials allowed/used, any protocol transactions that take place, and what constitutes a “successful logon”.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes the logon process for each logon method supported for the product. Upon investigation, the evaluator found that the TSS states that the TOE supports remote administration via SSH and local authentication via UART serial console. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5.3.2 FIA_UIA_EXT.1 TSS 2

Objective	The evaluator shall examine the TSS to determine that it describes which actions are allowed before user identification and authentication. The description shall cover authentication and identification for local and remote TOE administration.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes which actions are allowed before user identification and authentication. Upon investigation, the evaluator found that the TSS states that all administrator actions require authentication via the local or SSH console. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass when activity is complete

4.5.3.3 FIA_UIA_EXT.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in are described. For each supported the login method, the

	evaluator shall ensure the guidance documentation provides clear instructions for successfully logging on. If configuration is necessary to ensure the services provided before login are limited, the evaluator shall determine that the guidance documentation provides sufficient instruction on limiting the allowed services.
Evaluator Findings	The evaluator examined the AGD to verify that it describes any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in. Upon investigation, the evaluator found that the AGD describes the SSH configuration in "SSH Configuration Options" for instructions on how to configure the TOE's remote access methods and protocols. [AGD] section 7.3.2 describes how to set the administrator password for local console and remote password authentication. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5.4 FIA_UAU.7

4.5.4.1 FIA_UAU.7 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed.
Evaluator Findings	The evaluator examined the section titled Protection Authentication feedback in the AGD to verify that it describes any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed. Upon investigation, the evaluator found that the AGD states that the TOE does not display the password during authentication attempts.. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5.5 FIA_X509_EXT.1/Rev

4.5.5.1 FIA_X509_EXT.1/Rev TSS 1

Objective	The evaluator shall ensure the TSS describes where the check of validity of the certificates takes place, and that the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied). It is expected that revocation checking is performed when a certificate is used in an authentication step and when performing trusted updates (if selected). It is not necessary to verify the revocation status of X.509 certificates during power-up self-tests (if the option for using X.509 certificates for self-testing is selected).
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes where the check of validity of the certificates takes place, and that the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied). Upon investigation, the evaluator found that the TSS describes the validity checking of x509v3 certificates, including the full validation procedure. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5.5.2 FIA_X509_EXT.1/Rev TSS 2

Objective	The TSS shall describe when revocation checking is performed and on what certificates. If the revocation checking during authentication is handled differently depending on whether a full certificate chain or only a leaf certificate is being presented, any differences must be summarized in the TSS section and explained in the Guidance.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes when revocation checking is performed and on what certificates. Upon investigation, the evaluator found that the TSS does not state that validation is performed any differently depending on it being a LEAF or RootCA. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5.5.3 FIA_X509_EXT.1/Rev Guidance 1

Objective	The evaluator shall also ensure that the guidance documentation describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) and describes how certificate revocation checking is performed and on which certificate.
Evaluator Findings	The evaluator examined the section titled X509 Certificate Validation in the AGD to verify that it contains describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE and describes how certificate revocation checking is performed and on which certificate. Upon investigation, the evaluator found that the AGD describes when and how the TOE checks certificate validity, including the rules for validation. AGD does not identify any extendedKeyUsage fields which are not supported. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5.6 FIA_X509_EXT.2

4.5.6.1 FIA_X509_EXT.2 TSS 1

Objective	The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes how the TOE chooses which certificates to use. Upon investigation, the evaluator found that the TSS states that the TOE only supports one certificate. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5.6.2 FIA_X509_EXT.2 TSS 2

Objective	The evaluator shall examine the TSS to confirm that it describes the behaviour of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. The evaluator shall verify that any distinctions between trusted channels are described. If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the guidance documentation contains instructions on how this

	configuration action is performed.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes the behaviour of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. Upon investigation, the evaluator found that the TSS states that connections fail when the connection to a CRL cache cannot be established. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5.6.3 FIA_X509_EXT.2 Guidance 1

Objective	The evaluator shall check the administrative guidance to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates.
Evaluator Findings	The evaluator examined the section titled X509 Certificate Validation in the AGD to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates. Upon investigation, the evaluator found that the AGD describes all necessary configuration to generate keypairs and CSRs, and import signed certificates into the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5.6.4 FIA_X509_EXT.2 Guidance 2

Objective	If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the guidance documentation contains instructions on how this configuration action is performed.
Evaluator Findings	[ST] section 5.2.3.7 does not select any configurable options.
Verdict	Pass

4.5.6.5 FIA_X509_EXT.2 Guidance 3

Objective	The evaluator shall also ensure that the guidance documentation describes the configuration required in the operating environment so the TOE can use the certificates. The guidance documentation shall also include any required configuration on the TOE to use the certificates. The guidance document shall also describe the steps for the Security Administrator to follow if the connection cannot be established during the validity check of a certificate used in establishing a trusted channel.
Evaluator Findings	The evaluator examined the section titled X509 Certificate Validation in the AGD. Upon investigation, the evaluator found that the AGD describes the process for configuring the TOE to use certificates. [AGD] section 14.1 provides general guidance for what constitutes a valid certificate. [AGD] section 14.5 states that if the validity check cannot be completed, the connection will fail. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.5.7 FIA_X509_EXT.3

4.5.7.1 FIA_X509_EXT.3 TSS 1

Objective	If the ST author selects "device-specific information", the evaluator shall verify that the TSS contains a description of the device-specific fields used in certificate requests.
Evaluator Findings	[ST] section 5.2.3.8 does not select “device specific information”
Verdict	Pass

4.5.7.2 FIA_X509_EXT.3 Guidance 1

Objective	The evaluator shall check to ensure that the guidance documentation contains instructions on requesting certificates from a CA, including generation of a Certificate Request. If the ST author selects "Common Name", "Organization", "Organizational Unit", or "Country", the evaluator shall ensure that this guidance includes instructions for establishing these fields before creating the Certification Request.
Evaluator Findings	The evaluator examined the section titled X509 Certificate Validation in the AGD to verify that it contains instructions on requesting certificates from a CA, including generation of a Certification Request. Upon investigation, the evaluator found that the AGD describes the process for generating keypairs and CSRs, including the necessary fields. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.6 TSS and Guidance Activities (Security Management)

4.6.1 FMT_MOF.1/ManualUpdate

4.6.1.1 FMT_MOF.1/ManualUpdate Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary steps to perform manual update are described. The guidance documentation shall also provide warnings regarding functions that may cease to operate during the update (if applicable).
Evaluator Findings	The evaluator examined the section titled Manual Update Mode ***and “Software Update Instructions”*** in the AGD to verify that it describes any necessary steps to perform manual update. Upon investigation, the evaluator found that the AGD fully describes the steps and processes to update the TOE. The evaluator examined the section titled Manual Update Mode in the AGD to verify that it provides warnings regarding functions that may cease to operate during the update (if applicable). Upon investigation, the evaluator found that the AGD describes that the TOE must reboot to perform the update; this will necessarily stop and restart all services and functions of the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.6.2 FMT_FMT_MOF.1/Functions

4.6.2.1 FMT_MOF.1/Functions TSS 2

Objective	For non-distributed TOEs, the evaluator shall ensure the TSS for each administrative function

	identified the TSS details how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE).
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS identifies each administrative function identified the TSS details how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE). Upon investigation, the evaluator found that the TSS describes that the administrator modifies the behaviour of the TOE transmission of audit data by configuring a different destination. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.6.2.2 FMT_MOF.1/Functions Guidance 2

Objective	For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation describes how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE) are performed to include required configuration settings.
Evaluator Findings	The evaluator examined the section titled Protected Audit Event Storage in the AGD to verify that it describes how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE) are performed to include required configuration settings. Upon investigation, the evaluator found that the AGD describes all necessary configuration steps to change the destination of audit server logs to a new destination. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.6.3 FMT_MTD.1/CoreData

4.6.3.1 FMT_MTD.1/CoreData TSS 1

Objective	The evaluator shall examine the TSS to determine that, for each administrative function identified in the guidance documentation; those that are accessible through an interface prior to administrator log-in are identified. For each of these functions, the evaluator shall also confirm that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS identifies administrative functions that are accessible through an interface prior to administrator log-in. Upon investigation, the evaluator found that the TSS states that no administrator actions are available prior to authentication. The evaluator examined the section titled TSS in the Security Target to verify that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users. Upon investigation, the evaluator found that the TSS states that all administrator functions must be performed via an authenticated session at the local or remote

	console. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.6.3.2 FMT_MTD.1/CoreData TSS 2

Objective	If the TOE supports handling of X.509v3 certificates and implements a trust store, the evaluator shall examine the TSS to determine that it contains sufficient information to describe how the ability to manage the TOE's trust store is restricted.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that, if the TOE supports handling of X.509v3 certificates and implements a trust store, the TSS contains sufficient information to describe how the ability to manage the TOE's trust store is restricted. Upon investigation, the evaluator found that the TSS states that the TOE implements a trust store, use of which is fully described in [AGD]. Management of the trust store is an administrator function, and the TOE disallows all administrator functions to non-authenticated administrative users. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.6.3.3 FMT_MTD.1/CoreData Guidance 1

Objective	The evaluator shall review the guidance documentation to determine that each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP is identified, and that configuration information is provided to ensure that only administrators have access to the functions.
Evaluator Findings	The evaluator examined the AGD to verify that it identifies each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP. Upon investigation, the evaluator found that the AGD addresses all TSF-data-manipulating functions, including all configuration. AGD section 8 states that the TOE may only be administered by a properly identified and authenticated administrator via the remote or local console. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.6.3.4 FMT_MTD.1/CoreData Guidance 2

Objective	If the TOE supports handling of X.509v3 certificates and provides a trust store, the evaluator shall review the guidance documentation to determine that it provides sufficient information for the administrator to configure and maintain the trust store in a secure way. If the TOE supports loading of CA certificates, the evaluator shall review the guidance documentation to determine that it provides sufficient information for the administrator to securely load CA certificates into the trust store. The evaluator shall also review the guidance documentation to determine that it explains how to designate a CA certificate a trust anchor.
Evaluator Findings	The evaluator examined the section titled X509 Certificate Validation in the AGD to verify that, if the TOE supports handling of X.509v3 certificates and provides a trust store, it provides sufficient information for the administrator to configure and maintain the trust store in a secure way. Upon investigation, the evaluator found that the AGD fully describes the operation of the TOE trust store, including all steps necessary to add or remote certificates from the trust store,

	and indicate which certificate end-entity or trustedCA certificates. The evaluator examined the section titled X509 Certificate Validation in the AGD to verify that, if the TOE supports loading of CA certificates, it provides sufficient information for the administrator to securely load CA certificates into the trust store and that it explains how to designate a CA certificate a trust anchor. Upon investigation, the evaluator found that the AGD fully describes how certificates are handled in the certificate store, and how certificates are indicated as roots of trust. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.6.4 FMT_MTD.1/CryptoKeys

4.6.4.1 FMT_MTD.1/CryptoKeys TSS 2

Objective	For non-distributed TOEs, the evaluator shall ensure the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. Upon investigation, the evaluator found that the TSS describes that the administrator may create new keys or delete old keys via the underlaying operating system. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.6.4.2 FMT_MTD.1/CryptoKeys Guidance 2

Objective	For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.
Evaluator Findings	The evaluator examined the AGD to verify that it lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. Upon investigation, the evaluator found that the AGD describes management of X.509v3 keypairs in [AGD] section 14.2, management of ssh public keys for public-key authentication in [AGD] section 8.2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.6.5 FMT_SMF.1

4.6.5.1 FMT_SMF.1 TSS 1

Objective	The evaluator shall confirm that the TSS details which security management functions are available through which interface(s) (local administration interface, remote administration interface). The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface.

Evaluator Findings	The evaluator examined the section titled TSS in the TSS to verify that it details which security management functions are available through which interface(s). Upon investigation, the evaluator found that the TSS states that the TOE may be administered from the local or remote console.. The evaluator examined the section titled User Identification and Authentication in the AGD to verify that it describes the local administrative interface. Upon investigation, the evaluator found that the AGD describes that the TOE may be administered via the local or remote consoles. Both TSS and AGD describe the local console as a UART serial connection, and [AGD] provides specific connection information such as baud rate and error correction. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.6.5.2 FMT_SMF.1 Guidance 1

Objective	The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface. The evaluator shall ensure the Guidance Documentation includes appropriate warnings for the administrator to ensure the interface is local.
Evaluator Findings	The evaluator examined the section titled User Identification and Authentication in the AGD to verify that it describes the local administrative interface. Upon investigation, the evaluator found that the TSS states that the TOE may be administered from the local or remote console.. The evaluator examined the section titled User Identification and Authentication in the AGD to verify that it describes the local administrative interface. Upon investigation, the evaluator found that the AGD describes that the TOE may be administered via the local console. Both TSS and AGD describe the local console as a UART serial connection, and [AGD] provides specific connection information such as baud rate and error correction. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.6.6 FMT_SMF.1/VPN

4.6.6.1 FMT_SMF.1/VPN TSS

Objective	The evaluator shall examine the TSS to confirm that all management functions specified in FMT_SMF.1/VPN are provided by the TOE. As with FMT_SMF.1 in the Base-PP, the evaluator shall ensure that the TSS identifies what logical interfaces are used to perform these functions and that this includes a description of the local administrative interface.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS states that all management functions specified in FMT_SMF.1/VPN are provided by the TOE. Upon investigation, the evaluator found that the TSS states that all management functions specified in FMT_SMF.1/VPN are provided by the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.6.6.2 FMT_SMF.1/VPN Guidance

Objective	The evaluator shall examine the operational guidance to confirm that all management functions specified in FMT_SMF.1/VPN are provided by the TOE. As with FMT_SMF.1 in the Base-PP, the evaluator shall ensure that the operational guidance identifies what logical interfaces are used to perform these functions and that this includes a description of the local administrative interface.
Evaluator Findings	The evaluator examined the AGD to confirm that all management functions specified in FMT_SMF.1/VPN are provided by the TOE. Upon investigation, the evaluator found that the AGD fully describes the operation of the packet filtering and IPsec systems. [AGD] section 8 states that administration of the TOE may be performed or local or remote consoles. [AGD] section 2.6 indicates that the TOE must be managed from the "Red" or trusted network segment. [AGD] section 8.3 describes the local interface. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.6.7 FMT_SMR.2

4.6.7.1 FMT_SMR.2 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details the TOE supported roles and any restrictions of the roles involving administration of the TOE.
Evaluator Findings	The evaluator examined the section titled TSS in the TSS to verify that the TOE supported roles and any restrictions of the roles involving administration of the TOE. Upon investigation, the evaluator found that the TSS states that the TOE supports only one role, "Security Administrator". Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.6.7.2 FMT_SMR.2 Guidance 1

Objective	The evaluator shall review the guidance documentation to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration.
Evaluator Findings	The evaluator examined the section titled User Identification and Authentication in the AGD to verify that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration. Upon investigation, the evaluator found that the AGD fully describes the necessary steps prior to authentication (such as setting or changing passwords or configuring public key authentication). AGD fully describes both local and remote administration, via the UART serial connection or red-network SSH connection. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.7 TSS and Guidance Activities (Packet Filtering)

4.7.1 FPF_RUL_EXT.1

4.7.1.1 FPF_RUL_EXT.1.1 TSS 1

Objective	The evaluator shall verify that the TSS provide a description of the TOE's initialization/startup process, which clearly indicates where processing of network packets begins to take place, and provides a discussion that supports the assertion that packets cannot flow during this process. The evaluator shall verify that the TSS also includes a narrative that identifies the components (e.g., active entity such as a process or task) involved in processing the network packets and describes the safeguards that would prevent packets flowing through the TOE without applying the ruleset in the event of a component failure. This could include the failure of a component, such as a process being terminated, or a failure within a component, such as memory buffers full and cannot process packets.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS provides a description of the TOE's initialization/startup process and a discussion that supports the assertion that packets cannot flow during this process. Upon investigation, the evaluator found that the TSS describes the initialization process, and clearly indicates where network packet processing begins. [ST] asserts that no network packets may flow during this process. The evaluator examined the section titled TSS in the Security Target to verify that the TSS includes a narrative that identifies the components involved in processing the network packets and describes the safeguards that would prevent packets flowing through the TOE without applying the ruleset in the event of a component failure. Upon investigation, the evaluator found that the TSS describes the composition of the packet filtering system, and the layered safeguards against network packets flowing. The TOE is not distributed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.7.1.2 FPF_RUL_EXT.1.1 Guidance 1

Objective	The operational guidance associated with this requirement shall be assessed in the subsequent test assurance activities.
Evaluator Findings	The operational guidance associated with this requirement is assessed in the subsequent test assurance activities.
Verdict	Pass

4.7.1.3 FPF_RUL_EXT.1.4 TSS 1

Objective	The evaluator shall verify that the TSS describes a Packet Filtering policy that can use the following fields for each identified protocol, and that the RFCs identified for each protocol are supported:
	
	• IPv4 (RFC 791)
	  ○ Source address
	  ○ Destination Address
	  ○ Protocol
	• IPv6 (RFC 2460)
	  ○ Source address

	○ Destination Address ○ Next Header (Protocol) • TCP (RFC 793) ○ Source Port ○ Destination Port • UDP (RFC768) ○ Source Port ○ Destination Port The evaluator shall verify that the TSS describes how conformance with the identified RFCs has been determined by the TOE developer (e.g., third party interoperability testing, protocol compliance testing). The evaluator shall verify that each rule can identify the following actions: permit, discard, and log. The evaluator shall verify that the TSS identifies all interface types subject to the Packet Filtering policy and explains how rules are associated with distinct network interfaces. Where interfaces can be grouped into a common interface type (e.g., where the same internal logical path is used, perhaps where a common device driver is used) they can be treated collectively as a distinct network interface.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes a Packet Filtering policy, describes how conformance with the identified RFCs has been determined, each rule can identify the required actions, identifies all interface types subject to the Packet Filtering policy and explains how rules are associated with distinct network interfaces. Upon investigation, the evaluator found that the TSS describes the allowed parameters on which the TOE packet filter may operate, and includes IPv4, IPv6, Transport protocol or next-header, TCP or UDP service used, or network interface. For any rule or combination of rules, the TOE can be configured to encrypt, bypass in plain text, or discard any packet, with or without logging. TSS states that “network interfaces” are protected by packet filtering rules. TSS states that testing for RFC conformance is shown via regression and interoperability testing. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.7.1.4 FPF_RUL_EXT.1.4 Guidance 1

Objective	The evaluators shall verify that the operational guidance identifies the following protocols as being supported and the following attributes as being configurable within Packet filtering rules for the associated protocols: • IPv4 (RFC 791) ○ Source address ○ Destination Address ○ Protocol • IPv6 (RFC 2460) ○ Source address ○ Destination Address ○ Next Header (Protocol) • TCP (RFC 793) ○ Source Port

	○ Destination Port • UDP (RFC768) ○ Source Port ○ Destination Port The evaluator shall verify that the operational guidance indicates that each rule can identify the following actions: permit, discard, and log. The evaluator shall verify that the operational guidance explains how rules are associated with distinct network interfaces. The guidance may describe the other protocols contained within the ST (e.g., IPsec, IKE, potentially HTTPS, SSH, and TLS) that are processed by the TOE. The evaluator shall ensure that it is made clear what protocols were not considered as part of the TOE evaluation.
Evaluator Findings	The evaluator examined the section titled ***"Configuring Packet Filtering Rules"*** in the AGD to verify that it identifies the required protocols as being supported and the required attributes as being configurable within Packet filtering rules, indicates that each rule can identify the required actions, explains how rules are associated with distinct network interfaces, and makes clear what protocols were not considered as part of the TOE evaluation. Upon investigation, the evaluator found that the AGD describes all supported protocols, attributes, and actions and that this list conforms to the list in [ST] section 6. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.7.1.5 FPF_RUL_EXT.1.5 TSS 1

Objective	The evaluator shall verify that the TSS describes the algorithm applied to incoming packets, including the processing of default rules, determination of whether a packet is part of an established session, and application of administrator defined and ordered ruleset.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes the algorithm applied to incoming packets, including the processing of default rules, determination of whether a packet is part of an established session, and application of administrator defined and ordered ruleset. Upon investigation, the evaluator found that the TSS fully describes the chain of logic behind packet processing, including whether or not the packet is part of an established session, application of rules in order, and default-deny behavior if no matching rules are found. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.7.1.6 FPF_RUL_EXT.1.5 Guidance 1

Objective	The evaluator shall verify that the operational guidance describes how the order of Packet filtering rules is determined and provides the necessary instructions so that an administrator can configure the order of rule processing.
Evaluator Findings	The evaluator examined the section titled ***Configuring Packet Filtering Rules"*** in the AGD to verify that it describes how the order of Packet filtering rules is determined and provides the necessary instructions so that an administrator can configure the order of rule processing. Upon investigation, the evaluator found that the AGD describes that SPD rule ordering is governed by the Iptables entries, and instructs the administrator to place the rules in the

	desired sequence using the "rulenum" statement inside a new packet filter rule. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.7.1.7 FPF_RUL_EXT.1.6 TSS 1

Objective	The evaluator shall verify that the TSS describes the process for applying Packet filtering rules and also that the behavior (either by default, or as configured by the administrator) is to discard packets when there is no rule match.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes the process for applying Packet filtering rules and that the behavior is to deny packets when there is no rule match. Upon investigation, the evaluator found that the TSS states that the TOE will deny all packets which do not match any configured rules. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.7.1.8 FPF_RUL_EXT.1.6 TSS 2

Objective	The evaluator shall verify the TSS describes when the IPv4/IPv6 protocols supported by the TOE differ from the full list provided in the RFC Values for IPv4 and IPv6 table.
Evaluator Findings	The evaluator examined the section titled ***TSS*** in the Security Target to verify that the TSS describes when the IPv4/IPv6 protocols supported by the TOE differ from the full list provided in the RFC Values for IPv4 and IPv6 table. Upon investigation, the evaluator found that the TSS does not identify any variance between the IPv4/IPv6 protocols supported by the TOE and the full list of values in the RFCs. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.7.1.9 FPF_RUL_EXT.1.6 Guidance 1

Objective	The evaluator shall verify that the operational guidance describes the behavior if no rules or special conditions apply to the network traffic. If the behavior is configurable, the evaluator shall verify that the operational guidance provides the appropriate instructions to configure the behavior to discard packets with no matching rules.
Evaluator Findings	The evaluator examined the section titled "Dropping Packets" in the AGD to verify that it describes the behavior if no rules or special conditions apply to the network traffic. Upon investigation, the evaluator found that the AGD states that packets are dropped by default. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.7.1.10 FPF_RUL_EXT.1.6 Guidance 2

Objective	The evaluator shall verify that the operational guidance describes the range of IPv4/IPv6 protocols supported by the TOE.
Evaluator Findings	The evaluator examined the section titled ***Configuring Packet Filtering Rules"*** in the AGD to verify that it describes the range of IPv4/IPv6 protocols supported by the TOE. Upon investigation, the evaluator found that the AGD does not describe any variance between the

	IPv4/IPv6 protocols supported by the TOE and the full list of values in the RFCs. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.8 TSS and Guidance Activities (Protection of the TSF)

4.8.1 FPT_APW_EXT.1

4.8.1.1 FPT_APW_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details all authentication data that are subject to this requirement, and the method used to obscure the plaintext password data when stored. The TSS shall also detail passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS details all authentication data that are subject to this requirement and the method used to obscure the plaintext password data when stored. Upon investigation, the evaluator found that the TSS states that the TOE stores salted, hashed passwords in the underlying file system. The evaluator also examined the section titled TSS in the Security Target to verify that the TSS details that passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose. Upon investigation, the evaluator found that the TSS states that The TOE does not provide any interface which would allow a user or administrator to directly view the private portion of any key, or any password in plaintext. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.8.2 FPT_FLS.1/SelfTest

4.8.2.1 FPT_FLS.1/SelfTest TSS

Objective	The evaluator shall ensure the TSS describes how the TOE ensures a shutdown upon a self-test failure, a failed integrity check of the TSF executable image, or a failed health test of the noise source. If there are instances when a shut-down does not occur, (e.g., a failure is deemed non-security relevant), the evaluator shall ensure that those cases are identified and a rationale is provided that supports the classification and justificaties why the TOE's ability to enforce its security policies is not affected in any such instance.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes how the TOE ensures a shutdown upon a self-test failure, a failed integrity check of the TSF executable image, or a failed health test of the noise source. Upon investigation, the evaluator found that the TSS states that the TOE will halt and reboot in a safe mode if any self-test fails during updates. TSS states that the network-functions of the TOE will fail if any runtime self-test (such as cryptographic module self testing) were to fail, but while it would halt all protected communication with the TOE it would not cause the TOE to reboot without an administrator command. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

4.8.2.2 FPT_FLS.1/SelfTest Guidance

Objective	The evaluator shall verify that the operational guidance provides information on the self-test failures that can cause the TOE to shut down and how to diagnose the specific failure that has occurred, including possible remediation steps if available.
Evaluator Findings	The evaluator examined the section titled TSF Testing in the AGD to verify that it provides information on the self-test failures that can cause the TOE to shut down and how to diagnose the specific failure that has occurred. Upon investigation, the evaluator found that the AGD described the console output for successful and failed self-testing results, and describes the possible failure states of the cryptographic functionality tests. [AGD] section 10.2 instructs the administrator in remedial action to take when the TOE ceases normal operation. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.8.3 FPT_SKP_EXT.1

4.8.3.1 FPT_SKP_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details how any preshared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose. Upon investigation, the evaluator found that the [ST] does not include any pre-shared keys. [ST] Section 6.1 describes the storage location of private key portions of keypairs. TSS states that the TOE does not offer any interface which permits the private key to be directly viewed by any user or administrator. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.8.4 FPT_STM_EXT.1

4.8.4.1 FPT_STM_EXT.1 TSS 1 **[TD0632]**

Objective	The evaluator shall examine the TSS to ensure that it lists each security function that makes use of time, and that it provides a description of how the time is maintained and considered reliable in the context of each of the time related functions. If “obtain time from the underlying virtualization system” is selected, the evaluator shall examine the TSS to ensure that it identifies the VS interface the TOE uses to obtain time. If there is a delay between updates to the time on the VS and updating the time on the TOE, the TSS shall identify the maximum possible delay.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS lists each security function that makes use of time and provides a description of how the time is maintained and considered reliable in the context of each of the time related functions. Upon investigation, the evaluator found that the TSS describes the TSF which rely on correct time, and

	states that the TOE provides a realtime hardware clock with manual time setting and configuration by the administrator. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.8.4.2 FPT_STM_EXT.1 Guidance 1 **[TD0632]**

Objective	The evaluator examines the guidance documentation to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the guidance documentation instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication. If the TOE supports obtaining time from the underlying VS, the evaluator shall verify the Guidance Documentation specifies any configuration steps necessary. If no configuration is necessary, no statement is necessary in the Guidance Documentation. If there is a delay between updates to the time on the VS and updating the time on the TOE, the evaluator shall ensure the Guidance Documentation informs the administrator of the maximum possible delay.
Evaluator Findings	[ST] does not include FCS_NTP, nor any selection for FPT_STM_EXT which includes an NTP server or obtaining time from an underlying virtualization platform.
Verdict	Pass

4.8.5 FPT_TST_EXT.1.1

4.8.5.1 FPT_TST_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS details the self-tests that are run by the TSF on start-up. Upon investigation, the evaluator found that the TSS describes the self-tests performed by the TOE, and provides a justification for why the tests are believed to be sufficient to demonstrate correct operation of the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.8.5.2 FPT_TST_EXT.1.1 Guidance 1

Objective	The evaluator shall also ensure that the guidance documentation describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS.
Evaluator Findings	The evaluator examined the section titled TSF Testing in the AGD to verify that it describes the possible errors that may result from such tests, and actions the administrator should take in response. Upon investigation, the evaluator found that the AGD describes in detail the outcome of various self-tests, and the administrator actions to take in response to any failed self-tests. The evaluator verified that [AGD] and [ST] conform in their description of the self-testing.

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.8.6 FPT_TST_EXT.3

4.8.6.1 FPT_TST_EXT.3 TSS

Objective	The evaluator shall verify that the TSS describes the method used to perform self-testing on the TSF executable code, and that this method is consistent with what is described in the SFR.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes the method used to perform self-testing on the TSF executable code, and that this method is consistent with what is described in the SFR. Upon investigation, the evaluator found that the TSS describes performing a SHA based hash of the executable code, and comparing the result of the hash against a known value. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.8.7 FPT_TUD_EXT.1

4.8.7.1 FPT_TUD_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describe how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the TSS needs to describe how and when the inactive version becomes active. The evaluator shall verify this description.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes how to query the currently active version. Upon investigation, the evaluator found that the TSS describes the use of the “version_info” command to query the currently active version. TSS also states that the TOE does not use any form of delayed activation. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.8.7.2 FPT_TUD_EXT.1 TSS 2

Objective	The evaluator shall verify that the TSS describes all TSF software update mechanisms for updating the system firmware and software (for simplicity the term 'software' will be used in the following although the requirements apply to firmware and software). The evaluator shall verify that the description includes a digital signature verification of the software before installation and that installation fails if the verification fails. Alternatively, an approach using a published hash can be used. In this case the TSS shall detail this mechanism instead of the digital signature verification mechanism. The evaluator shall verify that the TSS describes the method by which the digital signature or published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the digital signature or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes all TSF software update mechanisms for updating the system software, includes a digital signature verification of the software before installation and that installation fails if the verification fails. Upon investigation, the evaluator found that the TSS describes manual checking for updates. Updates are verified via digital signature verification. TSS describes how

	updates are obtained, and the actions the TOE takes when the update candidate fails or succeeds in signature verification. Signature verification is RSA 4096. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.8.7.3 FPT_TUD_EXT.1 TSS 3

Objective	If the options 'support automatic checking for updates' or 'support automatic updates' are chosen from the selection in FPT_TUD_EXT.1.2, the evaluator shall verify that the TSS explains what actions are involved in automatic checking or automatic updating by the TOE, respectively.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS, if the options 'support automatic checking for updates' or 'support automatic updates' are chosen, explains what actions are involved in automatic checking or automatic updating by the TOE. Upon investigation, the evaluator found that the TSS describes administrators performing manual updates, and the TOE does not support automatic updates. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.8.7.4 FPT_TUD_EXT.1 TSS 5

Objective	If a published hash is used to protect the trusted update mechanism, then the evaluator shall verify that the trusted update mechanism does involve an active authorization step of the Security Administrator, and that download of the published hash value, hash comparison and update is not a fully automated process involving no active authorization by the Security Administrator. In particular, authentication as Security Administration according to FMT_MOF.1/ManualUpdate needs to be part of the update process when using published hashes.
Evaluator Findings	[ST] does not select "published hash" for trusted update verification.
Verdict	Pass

4.8.7.5 FPT_TUD_EXT.1 Guidance 1

Objective	The evaluator shall verify that the guidance documentation describes how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the guidance documentation needs to describe how to query the loaded but inactive version.
Evaluator Findings	The evaluator examined the section titled Manual Update Mode in the AGD to verify that it describes how to query the currently active version and, if a trusted update can be installed on the TOE with a delayed activation, the loaded but inactive version. Upon investigation, the evaluator found that the AGD describes how the current version is queried. ST states that the TOE does not support delayed activation of update images. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.8.7.6 FPT_TUD_EXT.1 Guidance 2

Objective	The evaluator shall verify that the guidance documentation describes how the verification of

	the authenticity of the update is performed (digital signature verification or verification of published hash). The description shall include the procedures for successful and unsuccessful verification. The description shall correspond to the description in the TSS.
Evaluator Findings	The evaluator examined the section titled ***Console Messages*** in the AGD to verify that it describes how the verification of the authenticity of the update is performed. Upon investigation, the evaluator found that the AGD describes the result of successful and unsuccessful signature verification, including the steps the administrator should take in response and which conforms to [ST] Section 6 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.8.7.7 FPT_TUD_EXT.1 Guidance 3

Objective	If a published hash is used to protect the trusted update mechanism, the evaluator shall verify that the guidance documentation describes how the Security Administrator can obtain authentic published hash values for the updates.
Evaluator Findings	[ST] does not select "published hashes" for trusted update verification.
Verdict	Pass

4.8.7.8 FPT_TUD_EXT.1 Guidance 6

Objective	If this was information was not provided in the TSS: If the ST author indicates that a certificate-based mechanism is used for software update digital signature verification, the evaluator shall verify that the Guidance Documentation contains a description of how the certificates are contained on the device. The evaluator also ensures that the Guidance Documentation describes how the certificates are installed/updated/selected, if necessary.
Evaluator Findings	[ST] does not select certificate-based update mechanisms in [ST] section 5.2.6.7
Verdict	Pass

4.9 TSS and Guidance Activities (TOE Access)

4.9.1 FTA_SSL_EXT.1

4.9.1.1 FTA_SSL_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details whether local administrative session locking or termination is supported and the related inactivity time period settings.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS identifies whether local administrative session locking or termination is supported and the related inactivity time period settings. Upon investigation, the evaluator found that the TSS describes that local administrative sessions are terminated when the timeout value elapses. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.9.1.2 FTA_SSL_EXT.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation states whether local administrative session locking or termination is supported and instructions for configuring the inactivity time period.
Evaluator Findings	The evaluator examined the section titled TSF-initiated Session Termination in the AGD to verify that it states whether local administrative session locking or termination is supported and instructions for configuring the inactivity time period. Upon investigation, the evaluator found that the AGD describes the local and remote timeout values, how to configure them, and states that the local or remote session will terminate when the inactivity timer elapses. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.9.2 FTA_SSL.3

4.9.2.1 FTA_SSL.3 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details the administrative remote session termination and the related inactivity time period.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS identifies administrative remote session termination and the related inactivity time period. Upon investigation, the evaluator found that the TSS describes that remote administrative sessions are terminated upon the elapse of the inactivity timer. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.9.2.2 FTA_SSL.3 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation includes instructions for configuring the inactivity time period for remote administrative session termination.
Evaluator Findings	The evaluator examined the section titled TSF-initiated session termination in the AGD to verify that it includes instructions for configuring the inactivity time period for remote administrative session termination. Upon investigation, the evaluator found that the AGD describes the remote console timeout value, provides instructions for configuring the value, and states that the remote console session will terminate when the timeout value elapses. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.9.3 FTA_SSL.3/VPN

4.9.4 FTA_SSL.4

4.9.4.1 FTA_SSL.4 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details how the local and remote administrative sessions are terminated.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS identifies details how the local and remote administrative sessions are terminated. Upon investigation, the evaluator found that the TSS describes the use of administrator-initiated

	termination of the local or remote sessions by using the CLI “logout” or “exit” commands. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.9.4.2 FTA_SSL.4 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation states how to terminate a local or remote interactive session.
Evaluator Findings	The evaluator examined the section titled User-Initiated Termination in the AGD to verify that it states how to terminate a local or remote interactive session. Upon investigation, the evaluator found that the AGD describes the use of the “Exit” or “logout” commands. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.9.5 FTA_TAB.1

4.9.5.1 FTA_TAB.1 TSS 1

Objective	The evaluator shall check the TSS to ensure that it details each administrative method of access (local and remote) available to the Security Administrator (e.g., serial port, SSH, HTTPS). The evaluator shall check the TSS to ensure that all administrative methods of access available to the Security Administrator are listed and that the TSS states that the TOE is displaying an advisory notice and a consent warning message for each administrative method of access. The advisory notice and the consent warning message might be different for different administrative methods of access and might be configured during initial configuration (e.g. via configuration file).
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS details each administrative method of access available to the Security Administrator and states that the TOE is displaying an advisory notice and consent warning message for each administrative method of access. Upon investigation, the evaluator found that the TSS describes the use of the local and remote consoles, and states that the configurable advisory notice and consent banner prior to authentication by administrators. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.9.5.2 FTA_TAB.1 Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure that it describes how to configure the banner message.
Evaluator Findings	The evaluator examined the section titled ***Default TOE Access Banner*** in the AGD to verify that it describes how to configure the banner message. Upon investigation, the evaluator found that the AGD describes the step for the administrator to configure an arbitrary advisory and consent notice banner on the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.10 TSS and Guidance Activities (Trusted Path/Channels)

4.10.1 FTP_ITC.1

4.10.1.1 FTP_ITC.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all secure communication mechanisms are described in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. Upon investigation, the evaluator found that the TSS describes the TOE as an IPsec peer and states that the TOE may accept or initiate IPsec communications via the trusted channel for other VPN endpoints or for the audit server communications. The evaluator examined the section titled TSS and Section 5.2.8.1 in the Security Target to verify that the TSS describes all secure communication mechanisms in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST. Upon investigation, the evaluator found that the TSS describes the IPsec functionality and it's TSF-enforcing functionality in sufficient detail to map the claimed TSF to the cryptographic protocols selected in [ST] section 5.2.2 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.10.1.2 FTP_ITC.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.
Evaluator Findings	The evaluator examined the section titled Configuring IPsec Parameters and Protected Audit Event Storage in the AGD to verify that it contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken. Upon investigation, the evaluator found that the AGD describes the IPsec communication parameters in sufficient detail for the administrator to configure the TOE to communicate with authorized IT entities. AGD 3.2 states that the TOE will attempt to send syslog traffic to the audit log server, and [AGD] 4.4.2 states how to configure the SPD such that traffic with the syslog server will be protected by IPsec. Should the connection be unintentionally broken, the TOE will continuously attempt to reestablish the IPsec tunnel to transmit audit logs. Should the IPsec connection be broken between the TOE and a Vpn peer, any traffic destined for the TOE or the Peer will trigger either the TOE or PEER to renegotiate the IPsec connection, automatically restoring the connection after a period of time as long as there is no interruption which would prevent it. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.10.2 FTP_ITC.1/VPN

4.10.2.1 FTP_ITC.1/VPN TSS 1

Objective	The evaluation activities specified for FTP_ITC.1 in the Supporting Document for the Base-PP shall be applied for IPsec VPN communications. From FTP_ITC.1: The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all secure communication mechanisms are described in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. Upon investigation, the evaluator found that the TSS describes that the TOE is a VPN peer, both client and server. Non-TSF endpoints are identified via their X.509v3 reference identifiers (FQDN, SAN, and/or CN). Allowed protocols are described, and are conformant with the selections made in [ST] Section 5.2.8.2 The evaluator examined the section titled TSS in the Security Target to verify that the TSS describes all secure communication mechanisms in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST. Upon investigation, the evaluator found that the TSS describes the TSFi and Ipsec functionality in sufficient detail to map the IPsec selections to the selections made in [ST] section 5.2.2 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.10.2.2 FTP_ITC.1/VPN Guidance 1

Objective	The evaluation activities specified for FTP_ITC.1 in the Supporting Document for the Base-PP shall be applied for IPsec VPN communications. From FTP_ITC.1: The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.
Evaluator Findings	The evaluator examined the section titled Configuring IPsec Parameters in the AGD to verify that it contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken. Upon investigation, the evaluator found that the AGD describes the IPsec communication parameters in sufficient detail for the administrator to configure the TOE to communicate with authorized IT entities. AGD 3.2 states that the TOE will attempt to send syslog traffic to the audit log server, and [AGD] 4.4.2 states how to configure the SPD such that traffic with the syslog server will be protected by IPsec. Should the connection be unintentionally broken, the TOE will continuously attempt to reestablish the IPsec tunnel to transmit audit logs. Should the IPsec connection be broken between the TOE and a Vpn peer, any traffic destined for the TOE

	or the Peer will trigger either the TOE or PEER to renegotiate the IPsec connection, automatically restoring the connection after a period of time as long as there is no interruption which would prevent it. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.10.3 FTP_TRP.1/Admin

4.10.3.1 FTP_TRP.1/Admin TSS 1

Objective	The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.
Evaluator Findings	The evaluator examined the section titled TSS in the Security Target to verify that the TSS indicates the methods of remote TOE administration and how those communications are protected. Upon investigation, the evaluator found that the TSS describes the TOE as an SSH server, which can accept trusted path communication from a remote administrator. The evaluator examined the section titled TSS in the Security Target to verify that the TSS protocols are consistent with those specified in the requirement. Upon investigation, the evaluator found that the TSS describes the SSH protocols in use by the TOE, which correspond to the selections made in [ST] section 5.2.2 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

4.10.3.2 FTP_TRP.1/Admin Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions for establishing the remote administrative sessions for each supported method.
Evaluator Findings	The evaluator examined the section titled SSH Configuration Options and Establishing Remote Administration Sessions in the AGD to verify that it contains instructions for establishing the remote administrative sessions for each supported method. Upon investigation, the evaluator found that the AGD describes the process for configuring the TOE's SSH server and establishing communication with the TOE over the trusted path. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5 Detailed Test Cases (Test Activities)

5.1 FAU_GEN.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the table of audit events and administrative actions listed above. This should include all instances of an event: for instance, if there are several different I&A mechanisms for a system, the FIA_UIA_EXT.1 events must be generated for each mechanism. The evaluator shall test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. If HTTPS is implemented, the test demonstrating the establishment and termination of a TLS session can be combined with the test for an HTTPS session. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the guidance documentation, and that the fields in each audit record have the proper entries. Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.
Test Steps	**Perform Testing**. Because testing of the TOE will exercise all functions, it is expected that the TOE will generate all audit logs.
Expected Test Results	**The TOE will generate audit event logs in the anticipated format.**
Pass/Fail with Explanation	Pass; the TOE correctly audits all claimed events.

5.2 FAU_STG_EXT.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing. The evaluator shall verify that the TOE is capable of transferring audit data to an external audit server automatically without administrator intervention.
Test Steps	• Establish a session between TOE and the audit server via IPsec. • Use Wireshark to examine the traffic between the TOE and the server. • Verify that the audit data is encrypted using the IPsec channel and reaches the audit server. • Record the name and version of the software the audit server uses during testing. • Attempt transfer audit data to external audit server without administrator prevention. • Attempt to delete audit data without administrative privilege. • Verify that transfer is successful by viewing the connection's pcap file.
Expected Test Results	Packet captures showing the TOE encrypts audit data sent between the TOE and the audit server.

	Log files showing the evaluator can transfer audit data to an external server without administrator intervention.
Pass/Fail with Explanation	Pass; channel data is not sent in plaintext.

5.3 FAU_STG_EXT.1 Test #2 (b)

Item	Data
Test Assurance Activity	Test 2: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behaviour defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that: The existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option '**overwrite previous audit records**' in FAU_STG_EXT.1.3)
Test Steps	• Check the /var/log/messages directory in the TOE's filesystem to see if the audit records are stored locally. • Generate enough audit data to the point where there is no storage left. • Attempt to write new audit record to the drive. • Verify that the oldest log entry has been overwritten with the new audit data by viewing log files.
Expected Test Results	Log files showing the TOE overwriting existing audit data when filled to maximum capacity.
Pass/Fail with Explanation	Pass; the TOE correctly enforced access controls on the audit data

5.4 FPT_STM_EXT.1 Test #1

Item	Data
Test Assurance Activity	Test 1: If the TOE supports direct **setting of the time by the Security Administrator** then the evaluator uses the guidance documentation to set the time. The evaluator shall then use an available interface to observe that the time was set correctly.
Test Steps	• SSH into the TOE and view the time. • Change the time of the TOE. • Verify the time displayed by the TOE is the one the user set. • View the log files to verify the change of time occurred.
Expected Test Results	Log files showing the administrator was able to set the time for the TOE.
Pass/Fail with Explanation	Pass; the TOE audited time changes

5.5 FTP_ITC.1 Test #1

Item	Data

Test Assurance Activity	The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
Test Steps	• Configure the TOE to use IPsec traffic. • Generate IPsec traffic and verify through packet captures. • Configure the TOE to send audit records to the syslog server over IPsec. • Generate audit records. • Verify that the audit records are encrypted via IPsec by viewing the log files.
Expected Test Results	Log files showing the TOE using IPsec to securely transfer data between itself and the syslog server.
Pass/Fail with Explanation	Pass; the TOE correctly protects audit data via the trusted channel

5.6 FTP_ITC.1 Test #2

Item	Data
Test Assurance Activity	For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE. (The TSF shall permit [*the authorized IT entities*] to initiate communication via the trusted channel.)
Test Steps	• Initiate IPsec connection from server to TOE • Send traffic to the TOE client. • Verify the ping was successful by viewing the log files. • Follow steps for all protocol supported.
Expected Test Results	Log files showing The TOE is able to have traffic sent to it.
Pass/Fail with Explanation	Pass; the TOE permits authorized IT entities to initiate communication via the trusted channel.

5.7 FTP_ITC.1 Test #3

Item	Data
Test Assurance Activity	The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.
Test Steps	This test is covered by FTP_ITC.1 Test #2
Expected Test Results	Log files showing the TOE can have traffic sent to it. Analysis of packet captures taken during this test demonstrates that syslog messages were not sent in plaintext.
Pass/Fail with Explanation	Pass; the TOE does not send trusted channel data in plaintext.

5.8 FTP_ITC.1 Test #4

Item	Data
Test Assurance Activity	Objective: The objective of this test is to ensure that the TOE reacts appropriately to any connection outage or interruption of the route to the external IT entities. The evaluator shall, for each instance where the TOE acts as a client utilizing a secure

	communication mechanism with a distinct IT entity, physically interrupt the connection of that IT entity for the following durations: 1. A duration that exceeds the TOE's application layer timeout setting, 2. A duration shorter than the application layer timeout but of sufficient length to interrupt the network link layer. The evaluator shall ensure that, when the physical connectivity is restored, communications are appropriately protected and no TSF data is sent in plaintext. In the case where the TOE is able to detect when the cable is removed from the device, another physical network device (e.g. a core switch) shall be used to interrupt the connection between the TOE and the distinct IT entity. The interruption shall not be performed at the virtual node (e.g. virtual switch) and must be physical in nature.
Test Steps	• Configure the TOE and Peer to use IPSec traffic. • Generate IPSec traffic and verify through packet captures that the traffic is encrypted. • Disconnect the network cable from the TOE for a short duration. • Reconnect network cable to TOE. • Verify traffic is still encrypted and session was resumed. • Disconnect the network cable from the TOE for a duration that exceeds the TOE's application layer timeout setting. • Reconnect network cable to TOE. • Verify traffic is encrypted and session was resumed after re-authentication.
Expected Test Results	PCAP files showing the TOE is able to properly encrypt network traffic in case of connection outage or interruption of route.
Pass/Fail with Explanation	Pass; the TOE did not send channel data in plaintext while the connection was broken, and successfully renegotiated the trusted channel after the connection was restored. Channel data were not sent in plaintext.

5.9 FCS_SSHS_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	Test 1: For each supported client public-key authentication algorithm, the evaluator shall configure a remote client to present a public key corresponding to that authentication method (e.g., 2048-bit RSA key when using ssh-rsa public key). The evaluator shall establish sufficient separate SSH connections with an appropriately configured remote non-TOE SSH client to demonstrate the use of all applicable public key algorithms. It is sufficient to observe the successful completion of the SSH Authentication Protocol to satisfy the intent of this test. **TD 0631 applied**.
Test Steps	1. Generate a new ecdsa-sha2-nistp384 private / public key pair for use by the test SSH client. 2. Load the ECDSA public key into the ToE authorized_keys file. 3. Run packet capture on pi-mercedes and attempt to SSH into the ToE at 10.0.41.1 using the generated key. 4. Verify that the successful authentication message was logged in the ToE's audit log.
Expected Test Results	• Client and server log files showing the remote client can securely connect to the TOE using the public key authentication algorithm specified in the ST (ecdsa-sha2-nistp384). • Packet captures showing the remote client can securely connect to the TOE using the public key authentication algorithm specified in the ST (ecdsa-sha2-nistp384).

Pass/Fail with Explanation	**Pass.** Authentication was successful with an ecdsa-sha2-nistp384 client key pair that the ToE was configured to accept. This was observable both from the client logs and the ToE's server logs, as well as independently from the packet capture.

5.10 FCS_SSHS_EXT.1.2 Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall choose one client public key authentication algorithm supported by the TOE. The evaluator shall generate a new client key pair for that supported algorithm without configuring the TOE to recognize the associated public key for authentication. The evaluator shall use an SSH client to attempt to connect to the TOE with the new key pair and demonstrate that authentication fails. TD 0631 applied.
Test Steps	1. Generate a new ecdsa-sha2-nistp384 private / public key pair for use by the test SSH client. 2. Run packet capture on pi-mercedes and attempt to SSH into the ToE at 10.0.41.1 using the generated key without having added it to the ToE's authorized_keys file. 3. Verify that the attempt from the client fails. 4. Verify that the failed attempt was recorded in the ToE's logs.
Expected Test Results	Client and server log files showing the remote client failed to authenticate with the untrusted ecdsa-sha2-nistp384 key.
Pass/Fail with Explanation	Pass. ToE successfully denies connection if a public / private ecdsa key pair that is not explicitly trusted by the ToE is used by a client. This was observable directly through both client and server logs.

5.11 FCS_SSHS_EXT.1.2 Test #3

Item	Data
Test Assurance Activity	Test 3: [Conditional] If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication succeeds when the correct password is provided by the connecting SSH client. **TD0631 has been applied.**
Pass/Fail with Explanation	This test is covered under by the steps performed and the evidence collected for FIA_UIA_EXT.1 Test #1, which demonstrates positive and negative testing for password authentication via SSH.

5.12 FCS_SSHS_EXT.1.2 Test #4

Item	Data
Test Assurance Activity	Test 4: [Conditional] If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication fails when the incorrect password is provided by the connecting SSH client. **TD0631 has been applied.**

Pass/Fail with Explanation	This test is covered under by the steps performed and the evidence collected for FIA_UIA_EXT.1 Test #1, which demonstrates positive and negative testing for password authentication via SSH.

5.13 FCS_SSHS_EXT.1.3 Test #1

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.
Test Steps	This test makes use of a python3 script and the AsyncSSH library to connect to the ToE using the trusted key generated in FCS_SSHS_EXT.1.2 Test #1. It opens an SSH channel on the authenticated connection, then crafts and sends a large SSHv2 packet of type 94 (SSH_MSG_CHANNEL_DATA) as defined in RFC4254. 1. While a packet capture is running on the interface to the ToE, run the python script from pi-mercedes. 2. Verify that when a packet that is larger than **262144 bytes** is sent over the SSH channel, it is dropped due to size by examining the ToE logs.
Expected Test Results	Log files showing the TOE can drop any packet that is above the specified size in the ST.
Pass/Fail with Explanation	**Pass.** The ToE rejects an SSHv2 packet that exceeds its maximum supported size of 262144 bytes. This event is recorded in the ToE's audit logs.

5.14 FCS_SSHS_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	The evaluator must ensure that only claimed ciphers and cryptographic primitives are used to establish an SSH connection. To verify this, the evaluator shall start session establishment for an SSH connection from a remote client (referred to as 'remote endpoint' below). The evaluator shall capture the traffic exchanged between the TOE and the remote endpoint during protocol negotiation (e.g. using a packet capture tool or information provided by the endpoint, respectively). The evaluator shall verify from the captured traffic that the TOE offers all the ciphers defined in the TSS for the TOE for SSH sessions, but no additional ones compared to the definition in the TSS. The evaluator shall perform one successful negotiation of an SSH session to verify that the TOE behaves as expected. It is sufficient to observe the successful negotiation of the session to satisfy the intent of the test. If the evaluator detects that not all ciphers defined in the TSS for SSH are supported by the TOE and/or the TOE supports one or more additional ciphers not defined in the TSS for SSH, the test shall be regarded as failed.
Test Steps	1. Ensure that the ToE is configured to only use the single encryption algorithm supported in the ST: aes256-gcm@openssh.com 2. Run a packet capture on pi-mercedes and attempt to SSH into the ToE at 10.0.41.1 from pi-mercedes with the client configured to use aes256-gcm@openssh.com. 3. Verify in the client logs that the ToE server offers only aes256-gcm@openssh.com, and no other ciphers as part of its KEXINIT proposal, and that aes256-gcm@openssh.com was successfully chosen as the negotiated cipher.

	4. Demonstrate that the negotiation of aes256-gcm@openssh.com was recorded in the ToE's logs. 5. Additionally demonstrate this from the packet capture collected during the negotiation.
Expected Test Results	• Log files showing the ToE can use the encryption algorithm defined in the ST to authenticate a connection with the TOE. • Packet capture validating that only the expected cipher (aes256-gcm@openssh.com) is offered and negotiated.
Pass/Fail with Explanation	**Pass.** TOE supports only the claimed cipher (aes256-gcm@openssh.com) during negotiation and is able to successfully form an encrypted channel with a client.

5.15 FCS_SSHS_EXT.1.5 Test #1

Item	Data
Test Assurance Activity	Test objective: This test case is meant to validate that the TOE server will support host public keys of the claimed algorithm types. Test 1: The evaluator shall configure (only if required by the TOE) the TOE to use each of the claimed host public key algorithms. The evaluator will then use an SSH client to confirm that the client can authenticate the TOE server public key using the claimed algorithm. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test. **TD 0631 applied**.
Pass/Fail with Explanation	**Pass.** This test is covered as a part of FCS_SSHS_EXT.1.2 Test #1 where the evaluator established sufficient separate SSH connections with an appropriately configured remote non-TOE SSH client to demonstrate the use of all applicable public key algorithms, since ecdsa-sha2-nistp384.

5.16 FCS_SSHS_EXT.1.5 Test #2

Item	Data
Test Assurance Activity	Test objective: This negative test case is meant to validate that the TOE Test objective: This negative test case is meant to validate that the TOE server does not support host public key algorithms that are not claimed. Test 2: The evaluator shall configure a non-TOE SSH client to only allow it to authenticate an SSH server host public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the non-TOE SSH client to the TOE SSH server and observe that the connection is rejected. **TD 0631 applied.**
Test Steps	1. Attempt to connect to the ToE from pi-mercedes' SSH Client using the trusted key generated in FCS_SSHS_EXT.1.2 Test #1, but configure the client to only authenticate an SSH server host public key algorithm of type ssh-ed25519, which is unsupported by the ToE. 2. Verify the authentication attempt fails in the client console logs due to an inability to negotiate host key type. 3. Verify that the ToE records the failed negotiation in its audit logs.
Expected Test Results	• Log files showing that the ToE was unable to negotiate with the test client for reason of incompatible host key algorithm, failing the connection.

	• Packet captures showing the client attempting to negotiate an unsupported algorithm (ssh-ed25519) and failing to establish an encrypted session.
Pass/Fail with Explanation	**Pass.** The client was unable to negotiate with the ToE when requesting an unsupported host key algorithm from the server. An SSH connection was not established.

5.17 FCS_SSHS_EXT.1.5 Test #3

Item	Data
Test Assurance Activity	Test 3: The evaluator shall configure an SSH client to only allow a public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the SSH client to the TOE and observe that the connection is rejected.
Test Steps	1. Generate a new ssh-ed25519 private / public key pair. 2. Attempt to connect to the ToE from pi-mercedes' SSH Client using the new key pair that is of a type unsupported by the ToE (ssh-ed25519). 3. Verify that the ToE fails to accept the client's publickey because of the type.
Expected Test Results	• Rejection of the SSHClient's attempt to authenticate with an unsupported public key algorithm type • Verification that the ToE has rejected the authentication attempt due to the client's unsupported pubkey.
Pass/Fail with Explanation	**Pass.** Authentication of the test client to the server fails because the client is attempting to use a public key algorithm type that is not supported by the ToE. This failure is logged as expected in the ToE's audit records.

5.18 FCS_SSHS_EXT.1.6 Test #1

Item	Data
Test Assurance Activity	Test 1: [conditional, if an **HMAC or AEAD_AES_*_GCM** algorithm is selected in the ST] The evaluator shall establish an SSH connection using each of the algorithms, except "implicit", specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test. Note: To ensure the observed algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.
Pass/Fail with Explanation	**N/A** This test requires the testing of all MAC algorithms except when aes256-gcm@openssh.com ciphers are used, since they are not associated with an explicitly negotiated MAC. This ToE only supports aes256-gcm@openssh.com for cipher algorithms, which are associated with the "implicit" type for HMAC and not covered by this test. Applying TD0446, this test is not applicable for this ToE.

5.19 FCS_SSHS_EXT.1.6 Test #2

Item	Data
Test Assurance Activity	Test 2: [conditional, if an **HMAC or AEAD_AES_*_GCM** algorithm is selected in the ST] The evaluator shall configure an SSH client to only allow a MAC algorithm that is not included in the

	ST selection. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails. Note: To ensure the proposed MAC algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.
Pass/Fail with Explanation	**N/A** This test requires the testing of all MAC algorithms except when aes256-gcm@openssh.com ciphers are used, since they are not associated with an explicitly negotiated MAC. This ToE only supports aes256-gcm@openssh.com for cipher algorithms, which are associated with the "implicit" type for HMAC and not covered by this test. Applying TD0446, this test is not applicable for this ToE.

5.20 FCS_SSHS_EXT.1.7 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure an SSH client to only allow the diffie-hellman-group1-sha1 key exchange. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.
Test Steps	1. Configure the SSH client on pi-mercedes to only allow the diffie-hellman-group1-sha1 kex algorithm and attempt to SSH into the ToE with otherwise valid credentials. Run a packet capture during the attempt. 2. Verify from the client console logs that the attempt fails for reason of failed key exchange negotiation. 3. Verify that this failed negotiation was recorded in the Toe's audit logs.
Expected Test Results	• Log files showing the TOE denies access from a user that is using a diffie-hellman-group1-sha1 key exchange. • Packet capture demonstrating that the ToE still attempts to negotiate only the supported algorithm (ecdh-sha2-nistp384).
Pass/Fail with Explanation	**Pass.** The ToE successfully refused the client's negotiation attempt because no compatible algorithm could be found.

5.21 FCS_SSHS_EXT.1.7 Test #2

Item	Data
Test Assurance Activity	For each allowed key exchange method, the evaluator shall configure an SSH client to only allow that method for key exchange, attempt to connect from the client to the TOE, and observe that the attempt succeeds.
Test Steps	For each key exchange method supported by the ToE. 1. Configure the SSH client on pi-mercedes to only allow the ecdh-sha2-nistp256 kex algorithm. 2. Verify that the key exchange successfully negotiates ecdh-sha2-nistp384 in the client console logs during the attempt, and that the client connects to the ToE. 3. Verify that the event was captured in the ToE's audit logs. 4. Configure the SSH client on pi-mercedes to only allow the ecdh-sha2-nistp384 kex algorithm and attempt to SSH into the ToE with valid credentials. Run a packet capture during the attempt.

	5. Verify that the key exchange successfully negotiates ecdh-sha2-nistp256 in the client console logs during the attempt, and that the client connects to the TOE. 6. Verify that the event was captured in the TOE's audit logs.
Expected Test Results	Log files showing the ToE allows the SSH client to connect to the TOE with the key exchange method ecdh-sha2-nistp384 and ecdh-sha2-nistp256, as defined in the ST. Packet capture verifying that the expected key exchange method is negotiated between the client and the ToE.
Pass/Fail with Explanation	**Pass.** For each supported key exchange method claimed, the ToE successfully authenticated with the properly configured SSH client peer and started an encrypted channel.

5.22 FCS_SSHS_EXT.1.8 Test #1

Item	Data
Test Assurance Activity	The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the **time-based threshold** and the traffic-based threshold. For testing of the time-based threshold, the evaluator shall use an SSH client to connect to the TOE and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator). Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one hour of session time but the value used for testing shall not exceed one hour. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE. If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions).
Test Steps	1. Configure the ToE for a threshold time value (5 seconds) for the time allowed for a key session, according to the guidance documentation. 2. Connect to the TOE via SSH and wait 18 seconds. 3. Keep the session open until the threshold is reached. 4. Verify that the session initiated a rekey. 5. Verify that the modification of rekey threshold requires administrative access. 6. Demonstrate that the configuration file for setting ssh configurations such as timeouts is restricted to root user write privileges.
Expected Test Results	• Log files showing the TOE initiates a rekey when the time threshold has elapsed. • Packet capture showing that over the duration of the connection, no period of network inactivity over SSH lasts longer than the configured timeout. • Observe that the privileges on the configuration file used for setting thresholds are limited to the root administrative user.
Pass/Fail with Explanation	**Pass.** The ToE can be configured to rekey SSH connections after a specified timeout and the rekeying at the specified interval can be observed in the logs, as initiated by the ToE. Additionally, this capability is limited to an administrative root user.

5.23 FCS_SSHS_EXT.1.8 Test #1b

Item	Data

Test Assurance Activity	The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the time-based threshold and the **traffic-based** threshold. For testing of the traffic-based threshold the evaluator shall use the TOE to connect to an SSH client and shall transmit data to and/or receive data from the TOE within the active SSH session until the threshold for data protected by either encryption key is reached. It is acceptable if the rekey occurs before the threshold is reached (e.g. because the traffic is counted according to one of the alternatives given in the Application Note for FCS_SSHS_EXT.1.8). The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator). Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one gigabyte of transferred traffic but the value used for testing shall not exceed one gigabyte. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE. If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions). In cases where data transfer threshold could not be reached due to hardware limitations it is acceptable to omit testing of this (SSH rekeying based on data transfer threshold) threshold if both the following conditions are met: 1. An argument is present in the TSS section describing this hardware- based limitation and All hardware components that are the basis of such argument are definitively identified in the ST. For example, if specific Ethernet Controller or WiFi radio chip is the root cause of such limitation, these chips must be identified.
Test Steps	1. Modify the SSH configuration to set the bytes to 1M and the time to 2700 seconds to trigger a byte-based rekey for this test, according to the guidance documentation. 2. Connect to the ToE from the ssh client peer on pi-mercedes with a new session and move bytes around. 3. Keep the session open until the threshold is reached. 4. Verify the ToE logs show the ToE initiating the rekey within the set byte limits before the long time limit has been exceeded. Note: Verification of administrative restriction is covered in FCS_SSHS_EXT.1.8 Test #1.
Expected Test Results	Log files showing the TOE initiates a rekey as the data thresholds are met. These intervals should be well below the timeout-based rekey which has been set high for this test.
Pass/Fail with Explanation	**Pass.** The ToE can be configured to rekey an SSH connection after a configurable number of bytes have been transferred. This is observed through the server-initiated rekeys seen in the audit logs that are within the byte-thresholds and well within the time thresholds, confirming the rekeys are not being triggered for time-based reasons.

5.24 FAU_GEN.1/VPN Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall attempt to flood the TOE with network packets such that the TOE will be unable to process all the packets. This may require the evaluator to configure the TOE to limit the bandwidth the TOE is capable to handling (e.g., use of a 10 MB interface). The evaluator shall then review the audit logs to verify that the TOE correctly records that it is unable to process all of the received packets and verify that the TOE logging behavior is consistent with the TSS.
Test Steps	• Follow guidance documentation to configure the TOE to limit the number of TCP connections. • Continually establish new TCP connections to the TOE until the limit is reached. • Verify the connections are permitted via packet capture. • Attempt to establish one more new TCP connection (above the limit). • Verify that the connection is denied via logs. Verify that the connection is denied via packet capture.
Expected Test Results	• The rule to limit the number of TCP connections is in place. • A packet capture shows a "SYN/SYN-ACK/ACK" handshake for new TCP connections until the limit is reached. • There is an "IPTABLES_DROPPED_PACKET" log for all "SYN" packets attempting to establish a new TCP connection once the limit is reached. • A packet capture shows a "SYN" packet (possibly retransmitted) without a response for all new TCP connections once the limit is reached.
Pass/Fail with Explanation	**PASS**. - Traffic was permitted before reaching the TOE's limitation. - When the TOE reached its limit, new connections were logged as "dropped" - The packet capture shows that a new connection could not be established after reaching the TOE's limitation.

5.25 FAU_GEN.1/VPN Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall use a remote VPN client to establish an IPsec session with the TOE and observe that the event is logged in accordance with the expectations of the PP-Module.
Test Steps	N/A.
Expected Test Results	N/A.
Pass/Fail with Explanation	This test is performed in conjunction with the FCS_IPSEC_EXT.1.1 Test #1. This meets the testing requirements.

5.26 FPF_RUL_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would otherwise be denied by the ruleset should be

	sourced and directed to a host. The evaluator shall use a packet sniffer to verify none of the generated network traffic is permitted through the TOE during initialization.
Test Steps	• Send continual ICMP traffic from 10.0.99.1 to 10.1.40.1 through the TOE. ○ This will be denied by the TOE's ruleset because it will not flow through an IPsec tunnel. • Verify that traffic is denied via packet capture. • While the continual ping is running, reboot the TOE. • Verify that packets are denied during reboot via packet capture. • Verify that packets are denied once the TOE is operational via packet capture.

Expected Test Results	• Ping logs on the remote machine shows:
	  ○ The TOE denying pings before the reboot.
	  ○ The TOE denying pings during the reboot.
	  ○ The TOE denying pings once the TOE is operational
	• A packet capture on the remote machine shows:
	  ○ The TOE denying pings before the reboot.
	  ○ The TOE denying pings during the reboot.
	  ○ The TOE denying pings once the TOE is operational.

Pass/Fail with Explanation	**PASS**. - The TOE denied traffic to flow through before the reboot. - During the reboot, the traffic (that would normally be denied by the TOE) was denied. - Once the TOE was operational again, the traffic was still denied by the TOE.

5.27 FPF_RUL_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would be permitted by the ruleset should be sourced and directed to a host. The evaluator shall use a packet sniffer to verify none of the generated network traffic is permitted through the TOE during initialization and is only permitted once initialization is complete.
Test Steps	• Follow guidance documentation to configure the TOE to negotiate a tunnel between 10.0.99.1/32 and 1.2.3.4/32 upon initialization. • Send continual ICMP traffic from 10.0.99.1 to 1.2.3.4 through the TOE. ○ This will be permitted by the TOE ruleset because it will flow through the IPsec tunnel. • Verify that traffic is permitted via packet capture. • While the continual ping is running, reboot the TOE. • Verify that packets are denied during reboot via packet capture. • Verify that packets are permitted once the TOE is operational via packet capture.
Expected Test Results	• Ping logs on the remote machine shows: ○ The TOE permitting pings before the reboot.

	○ The TOE denying pings during the reboot. ○ The TOE permitting pings once the TOE is operational • A packet capture on the remote machine shows: ○ The TOE permitting pings before the reboot. ○ The TOE denying pings during the reboot. ○ The TOE permitting pings once the TOE is operational.
Pass/Fail with Explanation	**PASS**. - The TOE permitted traffic to flow through before the reboot. - During the reboot, the traffic (that would normally flow through the TOE) was denied. - Once the TOE was operational again, the traffic was once again permitted to flow through the TOE.

5.28 FPF_RUL_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall use the instructions in the operational guidance to test that packet filter rules can be created that permit, deny, and log packets for each of the following attributes: • IPv4 ○ Source address ○ Destination Address ○ Protocol • IPv6 ○ Source address ○ Destination Address ○ Next Header (Protocol) • TCP ○ Source Port ○ Destination Port • UDP ○ Source Port ○ Destination Port Note that these test activities should be performed in conjunction with those of FPF_RUL_EXT.1.6 where the effectiveness of the rules is tested; here the evaluator is just ensuring the guidance is sufficient and the TOE supports the administrator creating a ruleset based on the above attributes. The test activities for FPF_RUL_EXT.1.6 define the protocol/attribute combinations required to be tested. If those combinations are configured manually, that will fulfill the objective of these test activities, but if those combinations are configured otherwise (e.g., using automation), these test activities may be necessary in order to ensure the guidance is correct and the full range of configurations can be achieved by a TOE administrator.
Test Steps	N/A
Expected Test Results	N/A

Pass/Fail with Explanation	This test is performed in conjunction with FPF_RUL_EXT.1.6, per the test assurance activity description. This meets the testing requirements.

5.29 FPF_RUL_EXT.1.4 Test #2

Item	Data
Test Assurance Activity	The evaluator shall repeat Test 1 above for each distinct network interface type supported by the TOE to ensure that Packet filtering rules can be defined for each all supported types. Note that these test activities should be performed in conjunction with those of FPF_RUL_EXT.1.6 where the effectiveness of the rules is tested; here the evaluator is just ensuring the guidance is sufficient and the TOE supports the administrator creating a ruleset based on the above attributes. The test activities for FPF_RUL_EXT.1.6 define the protocol/attribute combinations required to be tested. If those combinations are configured manually, that will fulfill the objective of these test activities, but if those combinations are configured otherwise (e.g., using automation), these test activities may be necessary in order to ensure the guidance is correct and the full range of configurations can be achieved by a TOE administrator.
Test Steps	N/A.
Expected Test Results	N/A.
Pass/Fail with Explanation	This test is performed in conjunction with FPF_RUL_EXT.1.6, per the test assurance activity description. This meets the testing requirements.

5.30 FPF_RUL_EXT.1.5 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall devise two equal Packet Filtering rules with alternate operations – permit and deny. The rules should then be deployed in two distinct orders and in each case the evaluator shall ensure that the first rule is enforced in both cases by generating applicable packets and using packet capture and logs for confirmation.

Test Steps	**TEST A ("permit" rule being first)**
	• Follow guidance documentation to configure two filters on the TOE.
	  ○ The first rule should log and **permit** packets from 1.0.0.1 to 3.0.0.1
	  ○ The first rule should log and **deny** packets from 1.0.0.1 to 3.0.0.1
	• Send traffic from 1.0.0.1 to 3.0.0.1 via the TOE.
	• Verify that traffic is permitted via logs.
	• Verify that traffic is permitted via packet capture.
	
	TEST B ("deny" rule being first)
	• Follow guidance documentation to configure two filters on the TOE.
	  ○ The first rule should log and **deny** packets from 1.0.0.1 to 3.0.0.1
	  ○ The first rule should log and **permit** packets from 1.0.0.1 to 3.0.0.1
	• Send traffic from 1.0.0.1 to 3.0.0.1 via the TOE.
	• Verify that traffic is denied via logs.

	• Verify that traffic is denied via packet capture.
Expected Test Results	**TEST A ("permit" rule being first)** • Show the "permit" rule is first. • There is an "IPTABLES_ACCEPTED_PACKET" log for all 5 packets sent from 1.0.0.1 to 3.0.0.1. • A packet capture on the TOE's in-interface shows all 5 packets. • A packet capture on the TOE's out-interface shows all 5 packets. **TEST B ("drop" rule being first)** • Show the "drop" rule is first. • There is an "IPTABLES_DROPPED_PACKET" log for all 5 packets sent from 1.0.0.1 to 3.0.0.1. • A packet capture on the TOE's in-interface shows all 5 packets. • A packet capture on the TOE's out-interface shows no packets.
Pass/Fail with Explanation	**PASS**. - When the "permit" rule was first, traffic was logged as accepted and captured on the TOE on the in-interface and on the out-interface. - When the "deny" rule was first, traffic was logged as denied and captured on the TOE on the in-interface but not on the out-interface.

5.31 FPF_RUL_EXT.1.5 Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall repeat the procedure above, except that the two rules should be devised where one is a subset of the other (e.g., a specific address vs. a network segment). Again, the evaluator should test both orders to ensure that the first is enforced regardless of the specificity of the rule.

Test Steps	**TEST A ("permit" rule being first)**
	• Follow guidance documentation to configure two filters on the TOE.
	  ○ The first rule should log and **permit** packets from 1.0.0.2 to 3.0.0.2
	  ○ The first rule should log and **deny** packets from 1.0.0.0/24 to 3.0.0.0/24
	• Send traffic from 1.0.0.2 to 3.0.0.2 via the TOE.
	• Verify that traffic is permitted via logs.
	• Verify that traffic is permitted via packet capture.
	
	TEST B ("deny" rule being first)
	• Follow guidance documentation to configure two filters on the TOE.
	  ○ The first rule should log and **deny** packets from 1.0.0.0/24 to 3.0.0.0/24
	  ○ The first rule should log and **permit** packets from 1.0.0.2 to 3.0.0.2
	• Send traffic from 1.0.0.2 to 3.0.0.2 via the TOE.
	• Verify that traffic is denied via logs.
	• Verify that traffic is denied via packet capture.

Expected Test Results	**TEST A ("permit" rule being first)** • Show the "permit" rule is first. • There is an "IPTABLES_ACCEPTED_PACKET" log for all 5 packets sent from 1.0.0.2 to 3.0.0.2. • A packet capture on the TOE's in-interface shows all 5 packets. • A packet capture on the TOE's out-interface shows all 5 packets. **TEST B ("drop" rule being first)** • Show the "drop" rule is first. • There is an "IPTABLES_DROPPED_PACKET" log for all 5 packets sent from 1.0.0.2 to 3.0.0.2. • A packet capture on the TOE's in-interface shows all 5 packets. • A packet capture on the TOE's out-interface shows no packets.
Pass/Fail with Explanation	**PASS**. - When the "permit" rule was first, traffic was logged as accepted and captured on the TOE on the in-interface and on the out-interface. - When the "deny" rule was first, traffic was logged as denied and captured on the TOE on the in-interface but not on the out-interface.

5.32 FPF_RUL_EXT.1.6 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall configure the TOE to permit and log each **supported** IPv4 Transport Layer Protocol (**see RFC Values for IPv4 and IPv6 table for full possible list**) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each **supported** IPv4 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that **the supported protocols** are permitted (i.e., by capturing the packets after passing through the TOE) and logged. **Any protocols not supported by the TOE must be denied.** **TD 0597 applied.**

Test Steps	**TEST A (single source/single destination)**
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **permit** packets of any protocol from 1.0.0.1/32 to 3.0.0.1/32.
	• Send traffic from 1.0.0.1 to 3.0.0.1 via the TOE.
	  ○ Ensure a packet is sent for each supported IPv4 protocol.
	• Verify that traffic is permitted via logs.
	• Verify that traffic is permitted via packet capture.
	
	TEST B (single source/wildcard destination)

	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **permit** packets of any protocol from 1.0.0.2/32 to 3.0.0.0/24.
	• Send traffic from 1.0.0.2 to 3.0.0.2 via the TOE.
	  ○ Ensure a packet is sent for each supported IPv4 protocol.
	• Verify that traffic is permitted via logs.
	• Verify that traffic is permitted via packet capture.
	
	TEST C (wildcard source/single destination)
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **permit** packets of any protocol from 1.0.0.0/24 to 3.0.0.3/32.
	• Send traffic from 1.0.0.3 to 3.0.0.3 via the TOE.
	  ○ Ensure a packet is sent for each supported IPv4 protocol.
	• Verify that traffic is permitted via logs.
	• Verify that traffic is permitted via packet capture.
	
	TEST D (wildcard source/wildcard destination)
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **permit** packets of any protocol from 1.0.0.0/24 to 3.0.0.0/24.
	• Send traffic from 1.0.0.4 to 3.0.0.4 via the TOE.
	  ○ Ensure a packet is sent for each supported IPv4 protocol.
	• Verify that traffic is permitted via logs.
	• Verify that traffic is permitted via packet capture.

Expected Test Results	**TEST A (single source/single destination)** • Show the “permit” rule is in place. • There is an “IPTABLES_ACCEPTED_PACKET” log for all 100 packets (each of different protocols) sent from 1.0.0.1 to 3.0.0.1. • A packet capture on the TOE’s in-interface shows all 100 packets. • A packet capture on the TOE’s out-interface shows all 100 packets. **TEST B (single source/wildcard destination)** • Show the “permit” rule is in place. • There is an “IPTABLES_ACCEPTED_PACKET” log for all 100 packets (each of different protocols) sent from 1.0.0.2 to 3.0.0.2. • A packet capture on the TOE’s in-interface shows all 100 packets. • A packet capture on the TOE’s out-interface shows all 100 packets. **TEST C (wildcard source/single destination)** • Show the “permit” rule is in place. • There is an “IPTABLES_ACCEPTED_PACKET” log for all 100 packets (each of different protocols) sent from 1.0.0.3 to 3.0.0.3.

	• A packet capture on the TOE's in-interface shows all 100 packets. • A packet capture on the TOE's out-interface shows all 100 packets. **TEST D (wildcard source/wildcard destination)** • Show the "permit" rule is in place. • There is an "IPTABLES_ACCEPTED_PACKET" log for all 100 packets (each of different protocols) sent from 1.0.0.4 to 3.0.0.4. • A packet capture on the TOE's in-interface shows all 100 packets. • A packet capture on the TOE's out-interface shows all 100 packets.
Pass/Fail with Explanation	**PASS**. - For each configuration, the "log and permit" rule correctly logged and permitted packets of every supported IPv4 protocol.

5.33 FPF_RUL_EXT.1.6 Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall configure the TOE to permit all traffic except to discard and log each **supported** IPv4 Transport Layer Protocol (**see RFC Values for IPv4 and IPv6 table for full possible list**) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv4 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that **the supported protocols** are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. **Any protocols not supported by the TOE must also be denied but are not required to be logged.** **TD 0597 applied.**

Test Steps	**TEST A (single source/single destination)**
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **drop** packets of any protocol from 1.0.0.1/32 to 3.0.0.1/32.
	• Follow guidance documentation to configure a filter to permit all other traffic.
	• Send traffic from 1.0.0.1 to 3.0.0.1 via the TOE.
	  ○ Ensure a packet is sent for each supported IPv4 protocol.
	• Verify that traffic is dropped via logs.
	• Verify that traffic is dropped via packet capture.
	
	TEST B (single source/wildcard destination)
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **drop** packets of any protocol from 1.0.0.2/32 to 3.0.0.0/24.
	• Follow guidance documentation to configure a filter to permit all other traffic.
	• Send traffic from 1.0.0.2 to 3.0.0.2 via the TOE.
	  ○ Ensure a packet is sent for each supported IPv4 protocol.
	• Verify that traffic is dropped via logs.

	• Verify that traffic is dropped via packet capture.
	
	TEST C (wildcard source/single destination)
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **drop** packets of any protocol from 1.0.0.0/24 to 3.0.0.3/32.
	• Follow guidance documentation to configure a filter to permit all other traffic.
	• Send traffic from 1.0.0.3 to 3.0.0.3 via the TOE.
	  ○ Ensure a packet is sent for each supported IPv4 protocol.
	• Verify that traffic is dropped via logs.
	• Verify that traffic is dropped via packet capture.
	
	TEST D (wildcard source/wildcard destination)
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **drop** packets of any protocol from 1.0.0.0/24 to 3.0.0.0/24.
	• Follow guidance documentation to configure a filter to permit all other traffic.
	• Send traffic from 1.0.0.4 to 3.0.0.4 via the TOE.
	  ○ Ensure a packet is sent for each supported IPv4 protocol.
	• Verify that traffic is dropped via logs.
	• Verify that traffic is dropped via packet capture.

Expected Test Results	**TEST A (single source/single destination)** • Show the "drop" rule is in place. • There is an "IPTABLES_DROPPED_PACKET" log for all 100 packets (each of different protocols) sent from 1.0.0.1 to 3.0.0.1. • A packet capture on the TOE's in-interface shows all 100 packets. • A packet capture on the TOE's out-interface shows no packets. **TEST B (single source/wildcard destination)** • Show the "drop" rule is in place. • There is an "IPTABLES_DROPPED_PACKET" log for all 100 packets (each of different protocols) sent from 1.0.0.2 to 3.0.0.2. • A packet capture on the TOE's in-interface shows all 100 packets. • A packet capture on the TOE's out-interface shows no packets. **TEST C (wildcard source/single destination)** • Show the "drop" rule is in place. • There is an "IPTABLES_DROPPED_PACKET" log for all 100 packets (each of different protocols) sent from 1.0.0.3 to 3.0.0.3. • A packet capture on the TOE's in-interface shows all 100 packets. • A packet capture on the TOE's out-interface shows no packets. **TEST D (wildcard source/wildcard destination)**

	• Show the "drop" rule is in place. • There is an "IPTABLES_DROPPED_PACKET" log for all 100 packets (each of different protocols) sent from 1.0.0.4 to 3.0.0.4. • A packet capture on the TOE's in-interface shows all 100 packets. • A packet capture on the TOE's out-interface shows no packets.
Pass/Fail with Explanation	**PASS**. - For each configuration, the "log and drop" rule correctly logged and dropped packets of every supported IPv4 protocol.

5.34 FPF_RUL_EXT.1.6 Test #3

Item	Data
Test Assurance Activity	Test 3: The evaluator shall configure the TOE to permit and log each **supported** IPv4 Transport Layer Protocol (**see RFC Values for IPv4 and IPv6 table for full possible list**) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. Additionally, the evaluator shall configure the TOE to discard and log each **supported** IPv4 Transport Layer Protocol (**see RFC Values for IPv4 and IPv6 table for full possible list**) in conjunction with different (than those permitted above) combinations of a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each **supported** IPv4 Transport Layer Protocol and outside the scope of all source and destination addresses configured above in order to ensure that **the supported protocols** are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. **Any protocols not supported by the TOE must be denied.** **TD 0597 applied.**

Test Steps	**TEST A (single source/single destination allow, single source/single destination deny)**
	• Follow guidance documentation to configure two filters on the TOE.
	  ○ This rule should log and **allow** packets of any protocol from 1.1.0.1/32 to 3.1.0.1/32.
	  ○ This rule should log and **drop** packets of any protocol from 1.2.0.1/32 to 3.2.0.1/32.
	• Follow guidance documentation to configure a filter to permit all other traffic.
	• Send traffic from 1.0.0.1 to 3.0.0.1 via the TOE.
	  ○ Ensure a packet is sent for each supported IPv4 protocol.
	• Verify that traffic is dropped via logs.
	• Verify that traffic is dropped via packet capture.
	
	Repeat the above tests with different IP addresses for all combinations as described in the test assurance activity.

Expected Test Results	For each configuration: • Show the "drop" rule is in place.

	• Show the "accept" rule is in place. • There is an "IPTABLES_DROPPED_PACKET" log for all packets (each of different protocols) sent from the testing addresses. • A packet capture on the TOE's in-interface shows all packets. • A packet capture on the TOE's out-interface shows no packets.
Pass/Fail with Explanation	**PASS**. - For each configuration, the default "log and drop" rule correctly logged and dropped packets of every supported IPv4 protocol that did not match a filtering rule.

5.35 FPF_RUL_EXT.1.6 Test #4

Item	Data
Test Assurance Activity	Test 4: The evaluator shall configure the TOE to permit and log each **supported** IPv6 Transport Layer Protocol (**see RFC Values for IPv4 and IPv6 table for full possible list**) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall **generate packets matching each defined IPv6 Transport Layer Protocol** and within the configured source and destination addresses in order to ensure that **the supported protocols** are **permitted (i.e., by capturing the packets after passing through the TOE) and logged**. **Any protocols not supported by the TOE must be denied.** **TD 0597 applied.**

Test Steps	**TEST A (single source/single destination)**
	• Follow guidance documentation to configure a filter on the TOE.
	  o This rule should log and **permit** packets of any protocol from 1::1 to 3::1.
	• Send traffic from 1::1 to 3::1 via the TOE.
	  o Ensure a packet is sent for each supported IPv6 protocol.
	• Verify that traffic is permitted via logs.
	• Verify that traffic is permitted via packet capture.
	
	TEST B (single source/wildcard destination)
	• Follow guidance documentation to configure a filter on the TOE.
	  o This rule should log and **permit** packets of any protocol from 1::2 to 3::/64.
	• Send traffic from 1::2 to 3::2 via the TOE.
	  o Ensure a packet is sent for each supported IPv6 protocol.
	• Verify that traffic is permitted via logs.
	• Verify that traffic is permitted via packet capture.
	
	TEST C (wildcard source/single destination)
	• Follow guidance documentation to configure a filter on the TOE.
	  o This rule should log and **permit** packets of any protocol from 1::/64 to 3::3.
	• Send traffic from 1::3 to 3::3 via the TOE.

	○ Ensure a packet is sent for each supported IPv6 protocol. • Verify that traffic is permitted via logs. • Verify that traffic is permitted via packet capture. **TEST D (wildcard source/wildcard destination)** • Follow guidance documentation to configure a filter on the TOE. ○ This rule should log and **permit** packets of any protocol from 1::/64 to 3::/64. • Send traffic from 1::4 to 3::4 via the TOE. ○ Ensure a packet is sent for each supported IPv6 protocol. • Verify that traffic is permitted via logs. • Verify that traffic is permitted via packet capture.
Expected Test Results	**TEST A (single source/single destination)** • Show the "permit" rule is in place. • There is an "IPTABLES_ACCEPTED_PACKET" log for all packets (each of different protocols) sent from 1::1 to 3::1. • A packet capture on the TOE's in-interface shows all packets. • A packet capture on the TOE's out-interface shows all packets. **TEST B (single source/wildcard destination)** • Show the "permit" rule is in place. • There is an "IPTABLES_ACCEPTED_PACKET" log for all packets (each of different protocols) sent from 1::2 to 3::2. • A packet capture on the TOE's in-interface shows all packets. • A packet capture on the TOE's out-interface shows all packets. **TEST C (wildcard source/single destination)** • Show the "permit" rule is in place. • There is an "IPTABLES_ACCEPTED_PACKET" log for all packets (each of different protocols) sent from 1::3 to 3::3. • A packet capture on the TOE's in-interface shows all packets. • A packet capture on the TOE's out-interface shows all packets. **TEST D (wildcard source/wildcard destination)** • Show the "permit" rule is in place. • There is an "IPTABLES_ACCEPTED_PACKET" log for all packets (each of different protocols) sent from 1::4 to 3::4. • A packet capture on the TOE's in-interface shows all packets. • A packet capture on the TOE's out-interface shows all packets.
Pass/Fail with Explanation	**PASS**. - For each configuration, the "log and permit" rule correctly logged and permitted packets of every supported IPv6 protocol.

5.36 FPF_RUL_EXT.1.6 Test #5

Item	Data
Test Assurance Activity	Test 5: The evaluator shall configure the TOE to permit all traffic except to discard and log each **supported** IPv6 Transport Layer Protocol (**see RFC Values for IPv4 and IPv6 table for full possible list**) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall **generate packets matching each defined IPv6 Transport Layer Protocol** and within the configured source and destination addresses in order to ensure that **the supported protocols are denied (i.e., by capturing no applicable packets passing through the TOE) and logged**. **Any protocols not supported by the TOE must also be denied but are not required to be logged.** **TD 0597 applied.**

Test Steps	**TEST A (single source/single destination)**
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **drop** packets of any protocol from 1::1 to 3::1.
	• Send traffic from 1::1 to 3::1 via the TOE.
	  ○ Ensure a packet is sent for each supported IPv6 protocol.
	• Verify that traffic is dropped via logs.
	• Verify that traffic is dropped via packet capture.
	
	TEST B (single source/wildcard destination)
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **drop** packets of any protocol from 1::2 to 3::/64.
	• Send traffic from 1::2 to 3::2 via the TOE.
	  ○ Ensure a packet is sent for each supported IPv6 protocol.
	• Verify that traffic is dropped via logs.
	• Verify that traffic is dropped via packet capture.
	
	TEST C (wildcard source/single destination)
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **drop** packets of any protocol from 1::/64 to 3::3.
	• Send traffic from 1::3 to 3::3 via the TOE.
	  ○ Ensure a packet is sent for each supported IPv6 protocol.
	• Verify that traffic is dropped via logs.
	• Verify that traffic is dropped via packet capture.
	
	TEST D (wildcard source/wildcard destination)
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **drop** packets of any protocol from 1::/64 to 3::/64.
	• Send traffic from 1::4 to 3::4 via the TOE.
	  ○ Ensure a packet is sent for each supported IPv6 protocol.
	• Verify that traffic is dropped via logs.
	• Verify that traffic is dropped via packet capture.

Expected Test Results	**TEST A (single source/single destination)** • Show the "drop" rule is in place. • There is an "IPTABLES_DROPPED_PACKET" log for all packets (each of different protocols) sent from 1::1 to 3::1. • A packet capture on the TOE's in-interface shows all packets. • A packet capture on the TOE's out-interface shows no packets. **TEST B (single source/wildcard destination)** • Show the "drop" rule is in place. • There is an "IPTABLES_DROPPED_PACKET" log for all packets (each of different protocols) sent from 1::2 to 3::2. • A packet capture on the TOE's in-interface shows all packets. • A packet capture on the TOE's out-interface shows no packets. **TEST C (wildcard source/single destination)** • Show the "drop" rule is in place. • There is an "IPTABLES_DROPPED_PACKET" log for all packets (each of different protocols) sent from 1::3 to 3::3. • A packet capture on the TOE's in-interface shows all packets. • A packet capture on the TOE's out-interface shows no packets. **TEST D (wildcard source/wildcard destination)** • Show the "drop" rule is in place. • There is an "IPTABLES_DROPPED_PACKET" log for all packets (each of different protocols) sent from 1::4 to 3::4. • A packet capture on the TOE's in-interface shows all packets. • A packet capture on the TOE's out-interface shows no packets.
Pass/Fail with Explanation	**PASS**. - For each configuration, the "log and drop" rule correctly logged and dropped packets of every supported IPv6 protocol.

5.37 FPF_RUL_EXT.1.6 Test #6

Item	Data
Test Assurance Activity	Test 6: The evaluator shall configure the TOE to permit and log each **supported** IPv6 Transport Layer Protocol (**see RFC Values for IPv4 and IPv6 table for full possible list**) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. Additionally, the evaluator shall configure the TOE to discard and log each **supported** IPv6 Transport Layer Protocol (**see RFC Values for IPv4 and IPv6 table for full possible list**) in conjunction with different (than those permitted above) combinations of a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and

	specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv6 Transport Layer Protocol and outside the scope of all source and destination addresses configured above in order to ensure that **the supported protocols** are dropped (i.e., by capturing no applicable packets passing through the TOE) and logged. **Any protocols not supported by the TOE must be denied.** **TD 0597 applied.**

Test Steps	**TEST A (single source/single destination allow, single source/single destination deny)**
	• Follow guidance documentation to configure two filters on the TOE.
	  ○ This rule should log and **allow** packets of any protocol from 1:1::1 to 3:1::1.
	  ○ This rule should log and **drop** packets of any protocol from 1:2.::1 to 3:2::1.
	• Follow guidance documentation to configure a filter to permit all other traffic.
	• Send traffic from 1::1 to 3::1 via the TOE.
	  ○ Ensure a packet is sent for each supported IPv6 protocol.
	• Verify that traffic is dropped via logs.
	• Verify that traffic is dropped via packet capture.
	
	Repeat the above tests with different IP addresses for all combinations as described in the test assurance activity.

Expected Test Results	For each configuration: • Show the "drop" rule is in place. • Show the "accept" rule is in place. • There is an "IPTABLES_DROPPED_PACKET" log for all packets (each of different protocols) sent from the testing addresses. • A packet capture on the TOE's in-interface shows all packets. A packet capture on the TOE's out-interface shows no packets.
Pass/Fail with Explanation	**PASS**. - For each configuration, the default "log and drop" rule correctly logged and dropped packets of every supported IPv6 protocol that did not match a filtering rule.

5.38 FPF_RUL_EXT.1.6 Test #7

Item	Data
Test Assurance Activity	Test 7: The evaluator shall configure the TOE to permit and log protocol 6 (TCP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination TCP ports in order to ensure that they are permitted (i.e., by capturing the packets after passing through the TOE) and logged.
Test Steps	**TEST A (selected source port)** • Follow guidance documentation to configure a filter on the TOE. ○ This rule should log and **permit** packets of TCP protocol with source port 498 between any addresses.

	• Send TCP traffic from 1.0.0.1:498 to 3.0.0.1:0 via the TOE.
	• Verify that traffic is permitted via logs.
	• Verify that traffic is permitted via packet capture.
	
	TEST B (selected destination port)
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **permit** packets of TCP protocol with destination port 499 between any addresses.
	• Send TCP traffic from 1.0.0.1:0 to 3.0.0.1:499 via the TOE.
	• Verify that traffic is permitted via logs.
	• Verify that traffic is permitted via packet capture.
	
	TEST C (selected source port and destination port)
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **permit** packets of TCP protocol with source port 500 and destination port 500 between any addresses.
	• Send TCP traffic from 1.0.0.1:500 to 3.0.0.1:500 via the TOE.
	• Verify that traffic is permitted via logs.
	• Verify that traffic is permitted via packet capture.

Expected Test Results	**TEST A (selected source port)** • Show the "permit" rule is in place. • There is an "IPTABLES_ACCEPTED_PACKET" log for the TCP packet sent from 1.0.0.1:498 to 3.0.0.1:0. • A packet capture on the TOE's in-interface shows the TCP packet. • A packet capture on the TOE's out-interface shows the TCP packet. **TEST B (selected source port)** • Show the "permit" rule is in place. • There is an "IPTABLES_ACCEPTED_PACKET" log for the TCP packet sent from 1.0.0.1:0 to 3.0.0.1:499. • A packet capture on the TOE's in-interface shows the TCP packet. • A packet capture on the TOE's out-interface shows the TCP packet. **TEST C (selected source port and destination port)** • Show the "permit" rule is in place. • There is an "IPTABLES_ACCEPTED_PACKET" log for the TCP packet sent from 1.0.0.1:500 to 3.0.0.1:500. • A packet capture on the TOE's in-interface shows the TCP packet. • A packet capture on the TOE's out-interface shows the TCP packet.
Pass/Fail with Explanation	**PASS**. - For each source/destination port configuration, the "log and permit" rule correctly logged and permitted TCP packets.

5.39 FPF_RUL_EXT.1.6 Test #8

Item	Data
Test Assurance Activity	Test 8: The evaluator shall configure the TOE to discard and log protocol 6 (TCP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination TCP ports in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged.

Test Steps	**TEST A (selected source port)**
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **deny** packets of TCP protocol with source port 498 between any addresses.
	• Send TCP traffic from 1.0.0.1:498 to 3.0.0.1:0 via the TOE.
	• Verify that traffic is denied via logs.
	• Verify that traffic is denied via packet capture.
	
	TEST B (selected destination port)
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **deny** packets of TCP protocol with destination port 499 between any addresses.
	• Send TCP traffic from 1.0.0.1:0 to 3.0.0.1:499 via the TOE.
	• Verify that traffic is denied via logs.
	• Verify that traffic is denied via packet capture.
	
	TEST C (selected source port and destination port)
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **deny** packets of TCP protocol with source port 500 and destination port 500 between any addresses.
	• Send TCP traffic from 1.0.0.1:500 to 3.0.0.1:500 via the TOE.
	• Verify that traffic is denied via logs.
	• Verify that traffic is denied via packet capture.

Expected Test Results	**TEST A (selected source port)** • Show the “drop” rule is in place. • There is an “IPTABLES_DROPPED_PACKET” log for the TCP packet sent from 1.0.0.1:498 to 3.0.0.1:0. • A packet capture on the TOE’s in-interface shows the TCP packet. • A packet capture on the TOE’s out-interface shows no TCP packet. **TEST B (selected source port)** • Show the “drop” rule is in place. • There is an “IPTABLES_DROPPED_PACKET” log for the TCP packet sent from 1.0.0.1:0 to 3.0.0.1:499. • A packet capture on the TOE’s in-interface shows the TCP packet. • A packet capture on the TOE’s out-interface shows no TCP packet.

	TEST C (selected source port and destination port) • Show the "drop" rule is in place. • There is an "IPTABLES_DROPPED_PACKET" log for the TCP packet sent from 1.0.0.1:500 to 3.0.0.1:500. • A packet capture on the TOE's in-interface shows the TCP packet. • A packet capture on the TOE's out-interface shows no TCP packet.
Pass/Fail with Explanation	**PASS**. - For each source/destination port configuration, the "log and drop" rule correctly logged and dropped TCP packets.

5.40 FPF_RUL_EXT.1.6 Test #9

Item	Data
Test Assurance Activity	Test 9: The evaluator shall configure the TOE to permit and log protocol 17 (UDP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination UDP ports in order to ensure that they are permitted (i.e., by capturing the packets after passing through the TOE) and logged. Here the evaluator ensures that the UDP port 500 (IKE) is included in the set of tests.

Test Steps	**TEST A (selected source port)**
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **permit** packets of UDP protocol with source port 498 between any addresses.
	• Send UDP traffic from 1.0.0.1:498 to 3.0.0.1:0 via the TOE.
	• Verify that traffic is permitted via logs.
	• Verify that traffic is permitted via packet capture.
	
	TEST B (selected destination port)
	• Follow guidance documentation to configure a filter on the UDP.
	  ○ This rule should log and **permit** packets of TCP protocol with destination port 499 between any addresses.
	• Send UDP traffic from 1.0.0.1:0 to 3.0.0.1:499 via the TOE.
	• Verify that traffic is permitted via logs.
	• Verify that traffic is permitted via packet capture.
	
	TEST C (selected source port and destination port)
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **permit** packets of UDP protocol with source port 500 and destination port 500 between any addresses.
	• Send UDP traffic from 1.0.0.1:500 to 3.0.0.1:500 via the TOE.
	• Verify that traffic is permitted via logs.
	• Verify that traffic is permitted via packet capture.

Expected Test Results	**TEST A (selected source port)**

	• Show the "permit" rule is in place. • There is an "IPTABLES_ACCEPTED_PACKET" log for the UDP packet sent from 1.0.0.1:498 to 3.0.0.1:0. • A packet capture on the TOE's in-interface shows the UDP packet. • A packet capture on the TOE's out-interface shows the UDP packet. **TEST B (selected source port)** • Show the "permit" rule is in place. • There is an "IPTABLES_ACCEPTED_PACKET" log for the UDP packet sent from 1.0.0.1:0 to 3.0.0.1:499. • A packet capture on the TOE's in-interface shows the UDP packet. • A packet capture on the TOE's out-interface shows the UDP packet. **TEST C (selected source port and destination port)** • Show the "permit" rule is in place. • There is an "IPTABLES_ACCEPTED_PACKET" log for the UDP packet sent from 1.0.0.1:500 to 3.0.0.1:500. • A packet capture on the TOE's in-interface shows the UDP packet. • A packet capture on the TOE's out-interface shows the UDP packet.
Pass/Fail with Explanation	**PASS**. - For each source/destination port configuration, the "log and permit" rule correctly logged and permitted UDP packets.

5.41 FPF_RUL_EXT.1.6 Test #10

Item	Data
Test Assurance Activity	Test 10: The evaluator shall configure the TOE to discard and log protocol 17 (UDP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination UDP ports in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. Again, the evaluator ensures that UDP port 500 is included in the set of tests.

Test Steps	**TEST A (selected source port)**
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **deny** packets of UDP protocol with source port 498 between any addresses.
	• Send TCP traffic from 1.0.0.1:498 to 3.0.0.1:0 via the TOE.
	• Verify that traffic is denied via logs.
	• Verify that traffic is denied via packet capture.
	
	TEST B (selected destination port)
	• Follow guidance documentation to configure a filter on the TOE.
	  ○ This rule should log and **deny** packets of UDP protocol with destination port 499 between any addresses.
	• Send TCP traffic from 1.0.0.1:0 to 3.0.0.1:499 via the TOE.
	• Verify that traffic is denied via logs.

	• Verify that traffic is denied via packet capture. **TEST C (selected source port and destination port)** • Follow guidance documentation to configure a filter on the TOE. ○ This rule should log and **deny** packets of UDP protocol with source port 500 and destination port 500 between any addresses. • Send UDP traffic from 1.0.0.1:500 to 3.0.0.1:500 via the TOE. • Verify that traffic is denied via logs. • Verify that traffic is denied via packet capture.
Expected Test Results	**TEST A (selected source port)** • Show the "drop" rule is in place. • There is an "IPTABLES_DROPPED_PACKET" log for the UDP packet sent from 1.0.0.1:498 to 3.0.0.1:0. • A packet capture on the TOE's in-interface shows the UDP packet. • A packet capture on the TOE's out-interface shows no UDP packet. **TEST B (selected source port)** • Show the "drop" rule is in place. • There is an "IPTABLES_DROPPED_PACKET" log for the UDP packet sent from 1.0.0.1:0 to 3.0.0.1:499. • A packet capture on the TOE's in-interface shows the UDP packet. • A packet capture on the TOE's out-interface shows no UDP packet. **TEST C (selected source port and destination port)** • Show the "drop" rule is in place. • There is an "IPTABLES_DROPPED_PACKET" log for the UDP packet sent from 1.0.0.1:500 to 3.0.0.1:500. • A packet capture on the TOE's in-interface shows the UDP packet. • A packet capture on the TOE's out-interface shows no UDP packet.
Pass/Fail with Explanation	**PASS**. - For each source/destination port configuration, the "log and drop" rule correctly logged and dropped TCP packets.

5.42 FCS_CKM.2 FCC is not included in the ST.

5.43 FIA_AFL.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application): Test 1: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE (and, if the time period selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall also use the operational

	guidance to configure the time period after which access is re-enabled). The evaluator shall test that once the authentication attempts limit is reached, authentication attempts with valid credentials are no longer successful.
Test Steps	• Configure the TOE to allow 3 unsuccessful login attempts. • Login to the TOE with an incorrect password 3 times. • Verify the TOE denied access to the user by viewing the log files. • Login to the TOE with the correct password. • Verify the TOE does not permit the user to login by viewing the log files.
Expected Test Results	Log files showing the user should not be able to login to the system after 3 incorrect login attempts for the specified amount of time.
Pass/Fail with Explanation	Pass; the TOE locks a user out when incorrect credentials are used too many times.

5.44 FIA_AFL.1 Test #2a is not a selection in the ST.

5.45 FIA_AFL.1 Test #2b

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application): Test 2: After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows: If the **time period** selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall wait for just less than the time period configured in Test 1 and show that an authorization attempt using valid credentials does not result in successful access. The evaluator shall then wait until just after the time period configured in Test 1 and show that an authorization attempt using valid credentials results in successful access.
Test Steps	• The evaluator configures the TOE to lock the user out for 1 minute. • Login with incorrect credentials 3 times to lock the user out. • Attempt to login with the correct credentials. • Verify the attempt is unsuccessful. • Attempt to login with the correct credentials after the time-out period has passed.
Expected Test Results	Log files showing the user should be able to login to the system after the time-out period has expired.
Pass/Fail with Explanation	Pass: the TOE correctly applied the timeout and session locking parameters as configured.

5.46 FIA_PMG_EXT.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall compose passwords that meet the requirements in some way. For each password, the evaluator shall verify that the TOE supports the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that all characters, and a minimum length listed in the requirement are supported and

	justify the subset of those characters chosen for testing.
Test Steps	• Configure the TOE so passwords must be at least 15 characters long, have an uppercase, a number, and a special character defined in the ST. • Create and test various passwords with permutations of allowed characters.
Expected Test Results	Administrator is able to configure passwords which meet the complexity requirements.
Pass/Fail with Explanation	Pass; the evaluator was able to configure password and authenticate to the TOE.

5.47 FIA_PMG_EXT.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall compose passwords that do not meet the requirements in some way. For each password, the evaluator shall verify that the TOE does not support the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that the TOE enforces the allowed characters and the minimum length listed in the requirement and justify the subset of those characters chosen for testing.
Test Steps	• Configure the TOE so passwords must be at least 15 characters long, have an uppercase, a number, and a special character defined in the ST. • Create and test various passwords with permutations of allowed characters.
Expected Test Results	Administrator is only able to configure passwords which meet the requirements and fails otherwise.
Test Output	This was tested in FIA_PMG_EXT.1 test1
Pass/Fail with Explanation	Pass; the administrator was able to set password requirements and the TOE enforced them

5.48 FIA_UIA_EXT.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 1: The evaluator shall use the guidance documentation to configure the appropriate credential supported for the login method. For that credential/login method, the evaluator shall show that providing correct I&A information results in the ability to access the system, while providing incorrect information results in denial of access.
Test Steps	• Attempt to login to the TOE remotely with correct credentials. • Verify that the TOE outputs the correct I&A information. • Attempt to login to the TOE remotely with incorrect credentials. • Verify that the TOE rejects the remote connection. • Repeat the same steps above but with local access.
Expected Test Results	Log files showing the TOE should grant access to the system when provided the correct credentials and denies access when given the wrong credentials.
Pass/Fail with Explanation	Pass; the TOE correctly rejected authentication attempts without the correct password, while allowing authentication with the correct password.

5.49 FIA_UIA_EXT.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 2: The evaluator shall configure the services allowed (if any) according to the guidance documentation, and then determine the services available to an external remote entity. The evaluator shall determine that the list of services available is limited to those specified in the requirement.
Test Steps	• Confirm that the only available service prior to authentication is the login banner. • Run netstat on TOE to check the available services.
Expected Test Results	The TOE should deny access to log files prior to authentication
Pass/Fail with Explanation	Pass; the TOE does not permit access to any TOE services except SSH, an authenticated service, and the local console.

5.50 FIA_UAU.7 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following test for each method of local login allowed: The evaluator shall locally authenticate to the TOE. While making this attempt, the evaluator shall verify that at most obscured feedback is provided while entering the authentication information.
Test Steps	• Attempt to locally login to the TOE. • Verify that output presented to user when logging in is obscured.
Expected Test Results	The TOE does not echo authentication data
Pass/Fail with Explanation	Pass; the TOE does not echo any authentication information at the local console.

5.51 FMT_MOF.1/AutoUpdate Test #1

Item	Data
Test Assurance Activity	The evaluator shall try to enable and disable automatic checking for updates or automatic updates (whichever is supported by the TOE) without prior authentication as Security Administrator (by authenticating as a user with no administrator privileges or without user authentication). The attempt to enable/disable automatic checking for updates should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to enable/disable automatic checking for updates can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps	The evaluator shall connect to the TOE and verify that unauthenticated users and non-administrators are not permitted to make changes.
Pass/Fail with Explanation	Pass; the TOE correctly rejected configuration changes from non-administrators.

5.52 FMT_MOF.1/AutoUpdate Test #2

Item	Data
Test Assurance Activity	The evaluator shall try to enable and disable automatic checking for updates or automatic updates (whichever is supported by the TOE) with prior authentication as Security Administrator. The attempt to enable/disable automatic checking for updates should be successful.
Test Steps	This test was performed as part of FPT_TST_EXT.1 and FPT_TUD_EXT.1
Pass/Fail with Explanation	Pass; the TOE permits the administrator to configure updates.

5.53 FMT_MOF.1/ManualUpdate Test #1

Item	Data
Test Assurance Activity	The evaluator shall try to perform the update using a legitimate update image without prior authentication as Security Administrator (either by authentication as a user with no administrator privileges or without user authentication at all – depending on the configuration of the TOE). The attempt to update the TOE shall fail.
Test Steps	• Disable Automatic Update mode. • Create new user with no administrative access. • Connect to the TOE as a non-administrator. Attempt to update the TOE and verify it rejects the request.
Expected Test Results	Log files showing the TOE should reject the request to update itself.
Pass/Fail with Explanation	Pass; the TOE rejects the request to update when user does not have administrative access.

5.54 FMT_MOF.1/ManualUpdate Test #2

Item	Data
Test Assurance Activity	The evaluator shall try to perform the update with prior authentication as Security Administrator using a legitimate update image. This attempt should be successful. This test case should be covered by the tests for FPT_TUD_EXT.1 already.
Test Steps	Performed as part of FPT_TUD_EXT.1
Expected Test Results	Performed as part of FPT_TUD_EXT.1
Pass/Fail with Explanation	Pass; the TOE permits the administrator to perform updates.

5.55 FMT_MOF.1/Functions (1) Test #1

Item	Data
Test Assurance Activity	Test 1 (if **'transmission of audit data to external IT entity'** is selected from the second selection together with **'modify the behaviour of'** in the first selection): The evaluator shall try to modify all security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). Attempts to modify parameters

	without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to modify the security related parameters can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps	• Connect to the TOE as a non-administrator. • Attempt to modify security parameters of configuration for transmission of audit data. • Verify that attempt is unsuccessful.
Expected Test Results	The TOE rejects unauthorized commands related to the IPsec trusted channel which protects audit data.
Pass/Fail with Explanation	Pass; the TOE correctly prevented non-administrators from changing any configuration related the security of audit data.

5.56 FMT_MOF.1/Functions (1) Test #2

Item	Data
Test Assurance Activity	Test 2 (if **'transmission of audit data to external IT entity'** is selected from the second selection together with **'modify the behaviour of'** in the first selection): The evaluator shall try to modify all security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity with prior authentication as Security Administrator. The effects of the modifications should be confirmed. The evaluator does not have to test all possible values of the security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity but at least one allowed value per parameter.
Test Steps	• N/A
Expected Test Results	N/A
Pass/Fail with Explanation	Pass; the TOE permits the administrator to test

5.57 FMT_MTD.1/CryptoKeys Test #1

Item	Data
Test Assurance Activity	The evaluator shall try to perform at least one of the related actions (modify, delete, generate/import) without prior authentication as Security Administrator (either by authentication as a non-administrative user, if supported, or without authentication at all). Attempts to perform related actions without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to manage cryptographic keys can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps	• Login to the TOE as a non-administrator. • Attempt to modify, delete, generate/import cryptographic keys on the TOE. • Verify the attempt was unsuccessful.
Expected Test Results	The TOE prevents non-administrators from modifying cryptographic keys.

Pass/Fail with Explanation	Pass; the TOE prevents non-administrators from making configuration changes to the keys on the TOE.

5.58 FMT_MTD.1/CryptoKeys Test #2

Item	Data
Test Assurance Activity	The evaluator shall try to perform at least one of the related actions with prior authentication as Security Administrator. This attempt should be successful.
Test Steps	• n/a
Expected Test Results	n/a
Pass/Fail with Explanation	Pass; the TOE permits administrators to configure the keys on the TOE.

5.59 FMT_SMF.1 Test #1

Item	Data
Test Assurance Activity	The evaluator tests management functions as part of testing the SFRs identified in section 2.4.4. No separate testing for FMT_SMF.1 is required unless one of the management functions in FMT_SMF.1.1 has not already been exercised under any other SFR.
Test Steps	Verify that the administrator can set the time All other TOE functions are tested in other SFRs and test steps.
Expected Test Results	The TOE accepts the updated time from the administrator.
Pass/Fail with Explanation	Pass; the administrator was able to set the time.

5.60 FMT_SMR.2 Test #1

Item	Data
Test Assurance Activity	In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, that each supported method of administering the TOE that conforms to the requirements of this cPP be tested; for instance, if the TOE can be administered through a local hardware interface; SSH; and TLS/HTTPS; then all three methods of administration must be exercised during the evaluation team's test activities.
Test Steps	Perform CC testing
Expected Test Results	The Evaluator is able to administer the TOE via the remote and local interfaces.
Pass/Fail with Explanation	Pass; the TOE permits the administrator to configure and operate the TOE via all supported interfaces.

5.61 FTA_SSL.3 Test #1

Item	Data

Test Assurance Activity	The evaluator shall follow the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.
Test Steps	• Configure a specific time to terminate a remote session after inactivity. • Login to TOE remotely and wait the specified time. • Verify that session is terminated after specified time.
Expected Test Results	The TOE terminates the local session after the timeout value.
Pass/Fail with Explanation	Pass; The TOE correctly terminated the session after the timeout period elapsed

5.62 FTA_SSL.4 Test #1

Item	Data
Test Assurance Activity	The evaluator shall initiate an interactive local session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Test Steps	• Login to the TOE locally as an administrator. • Disconnect from the TOE by the method described in the ST. • Verify the session gets terminated.
Expected Test Results	TOE exits the interactive session when requested by the administrator
Pass/Fail with Explanation	Pass; the TOE permitted the administrator to exit the local session

5.63 FTA_SSL.4 Test #2

Item	Data
Test Assurance Activity	The evaluator shall initiate an interactive remote session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Test Steps	• Login to the TOE remotely as an administrator. • Disconnect from the TOE by the method described in the ST. • Verify the session gets terminated.
Expected Test Results	The administrator is able to terminate their own session
Pass/Fail with Explanation	Pass; the administrator was able to quit the interactive remote session.

5.64 FTA_SSL_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes that the

	session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that reauthentication is needed when trying to unlock the session.
Test Steps	• Configure the TOE's inactivity period to 1 minute. • Start a local session with the TOE. • Verify that the session is terminated after 1 minute. • Repeat steps 1 through 3 with different inactivity periods.
Expected Test Results	Verify that the TOE terminates the session at the timeout value.
Pass/Fail with Explanation	Pass; the TOE correctly enforced the timeouts, and accepted administrator updated timeout values.

5.65 FTA_TAB.1 Test #1

Item	Data
Test Assurance Activity	The evaluator follows the guidance documentation to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify that the notice and consent warning message is displayed in each instance.
Test Steps	• Create a notice and consent warning message for users who are trying to access the TOE. • Attempt to connect to the TOE remotely. • Verify the warning message is displayed.
Expected Test Results	Log files showing the TOE should display the warning banner at both login screens.
Pass/Fail with Explanation	Pass; the TOE updated the banner and displayed it at the local and remote administrative session.

5.66 FTP_TRP.1/Admin Test #1

Item	Data
Test Assurance Activity	The evaluators shall ensure that communications using each specified (in the guidance documentation) remote administration method is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
Test Steps	• n/a
Expected Test Results	n/a
Pass/Fail with Explanation	Pass; the administrator is able to use the trusted path to administer the TOE.

5.67 FTP_TRP.1/Admin Test #2

Item	Data
Test Assurance Activity	The evaluator shall ensure, for each communication channel, the channel data is not sent in plaintext.
Test Steps	• na
Expected Test Results	n/a
Pass/Fail with Explanation	Pass; the TOE protects all communication via the trusted channel, and channel data are not set in plaintext.

5.68 FIA_X509_EXT.1.1/Rev Test #1a

Item	Data
Test Assurance Activity	Test 1a: The evaluator shall present the TOE with a valid chain of certificates (terminating in a trusted CA certificate) as needed to validate the leaf certificate to be used in the function and shall use this chain to demonstrate that the function succeeds. Test 1a shall be designed in a way that the chain can be 'broken' in Test 1b by either being able to remove the trust anchor from the TOEs trust store, or by setting up the trust store in a way that at least one intermediate CA certificate needs to be provided, together with the leaf certificate from outside the TOE, to complete the chain (e.g. by storing only the root CA certificate in the trust store).
Test Steps	• Upload a full certificate chain to the TOE • Verify that a log was generated when uploading the certificate change • Attempt an IPsec connection from the TOE to the configured remote IKEv2 peer and verify the connection is established using packet capture • Verify the connection is established using logs
Expected Test Results	the TOE will use X.509v3 certificates to establish the trusted channel
Pass/Fail with Explanation	Pass; the TOE established the trusted channel using X.509v3 certificates.

5.69 FIA_X509_EXT.1.1/Rev Test #1b

Item	Data
Test Assurance Activity	Test 1b: The evaluator shall then 'break' the chain used in Test 1a by either removing the trust anchor in the TOE's trust store used to terminate the chain, or by removing one of the intermediate CA certificates (provided together with the leaf certificate in Test 1a) to complete the chain. The evaluator shall show that an attempt to validate this broken chain fails.
Test Steps	• Begin with Test 1a and remove the root certificate from the TOE's trust store. • Attempt to connect from the TOE to IKEv2 peer and verify that the connection fails using packet capture • Verify that the connection fails using log
Expected Test Results	The TOE does not establish the connection when the trust chain is broken.
Pass/Fail with Explanation	Pass; the TOE did not establish the trusted channel session when the certificate trust chain was broken

5.70 FIA_X509_EXT.1.1/Rev Test #2

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.
Test Steps	• Create a certificate for a IKEv2 peer with a very short lifetime which is expired • Attempt to connect from the TOE to IKEv2 peer and verify the connection is refused using packet capture • Verify the connection is refused using logs
Expected Test Results	The TOE performs validity checking when the certificate is presented during trusted channel authentication
Pass/Fail with Explanation	Pass; the TOE correctly validated the certificate and trust chain during session establishment

5.71 FIA_X509_EXT.1.1/Rev Test #3

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 3: The evaluator shall test that the TOE can properly handle revoked certificates-–conditional on whether CRL or OCSP is selected; if both are selected, then a test shall be performed for each method. The evaluator shall test revocation of the peer certificate and revocation of the peer intermediate CA certificate i.e. the intermediate CA certificate should be revoked by the root CA. The evaluator shall ensure that a valid certificate is used, and that the validation function succeeds. The evaluator then attempts the test with a certificate that has been revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails. Revocation checking is only applied to certificates that are not designated as trust anchors. Therefore, the revoked certificate(s) used for testing shall not be a trust anchor.
Test Steps	Part 1 • Revoke an intermediate certificate in the uploaded certificate chain • Start the connection and verify the connection is not established using packet capture • Verify the connection is denied using logs Part 2 • Revoke the leaf certificate of the IKEv2 peer to which the TOE will be connecting • Attempt a connection from the TOE to the configured peer and verify the connection is not established using packet capture • Verify the connection is using logs

Expected Test Results	The TOE rejects session establishment when any part of the certificate trust chain is revoked.
Pass/Fail with Explanation	Pass, the TOE correctly rejected session establishment when any part of the trust chain is revoked.

5.72 FIA_X509_EXT.1.1/Rev Test #4

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. If OCSP is selected, the evaluator shall configure the OCSP server or use a man-in-the-middle tool to present a certificate that does not have the OCSP signing purpose and verify that validation of the OCSP response fails. If CRL is selected, the evaluator shall configure the CA to sign a CRL with a certificate that does not have the cRLsign key usage bit set and verify that validation of the CRL fails.
Test Steps	• Create a CRL that is signed by a certificate that does not have the CRLsign key usage bit set • Upload a full certificate chain to the TOE • Attempt to connect to the TOE to the TLS server and verify that the TOE rejected the connection using logs • Verify that the TOE rejected the connection using packet capture
Expected Test Results	The TOE rejects connections when the TOE cannot validate the CRL-signing bit in the issuer certificate.
Pass/Fail with Explanation	Pass; the TOE correctly rejected the connection when the CRL signer could not be trusted.

5.73 FIA_X509_EXT.1.1/Rev Test #5

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)
Test Steps	• Load certificate onto TOE • Modify first 8 bytes of the certificate and attempt to connect. The TOE will reject connection. • Verify TOE rejects modified certificate via packet capture
Expected Test Results	TOE successfully reject modified certificate.
Pass/Fail with Explanation	Pass. The TOE successfully rejected certificate with modified bytes.

5.74 FIA_X509_EXT.1.1/Rev Test #6

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. The evaluator shall modify any byte in the certificate signatureValue field (see RFC5280 Sec. 4.1.1.3), which is normally the last field in the certificate, and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)
Test Steps	• Run the StrongSwan Acumen tool to modify the last byte of the encoding certificate. • Verify that the TOE rejects the connection using TOE logs. • Verify that the TOE rejects the connection using packet capture.
Expected Test Results	The TOE rejects connections
Pass/Fail with Explanation	Pass; the TOE correctly rejected connection attempts when the certificate was invalid.

5.75 FIA_X509_EXT.1.1/Rev Test #7

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 7: The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The hash of the certificate will not validate.)
Test Steps	• Run the StrongSwan Acumen tool to modify any byte in public key of certificate. • Verify that the TOE rejects the connection using TOE logs. • Verify that the TOE rejects the connection using packet capture.
Expected Test Results	The TOE rejects the certificate when it is invalid
Pass/Fail with Explanation	Pass; the TOE correctly rejected the certificate.

5.76 FIA_X509_EXT.1.1/Rev Test #8c

Item	Data
Test Assurance Activity	**(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)** **(Conditional on support for a minimum certificate path length of three certificates)** The evaluator shall establish a subordinate CA certificate, where the elliptic curve parameters are specified as a named curve, that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is accepted into the TOE's trust store. The evaluator shall then establish a subordinate CA certificate that uses an explicit format version of the elliptic curve parameters, and that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is rejected, and not added to the TOE's trust store. **TD0527 (12/1 Update) has been applied.**
Test Steps	• Add a subordinate CA certificate into a TOE's trust store, where the elliptic curve parameters are specified as a named curve, that is signed by a trusted EC root CA.

	• Verify that the TOE accepts the certificate using TOE logs. • Add a subordinate CA certificate into a TOE's trust store, that uses an explicit format version of the elliptic curve parameters, and that is signed by a trusted EC root CA. • Verify that the TOE rejects the certificate using TOE logs.
Expected Test Results	The TOE rejects the improper certificate.
Pass/Fail with Explanation	Pass; the TOE rejected the improper certificate.

5.77 FIA_X509_EXT.1.2/Rev Test #1

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) then the associated extendedKeyUsage rule testing may be omitted. The goal of the following tests is to verify that the TOE accepts a certificate as a CA certificate only if it has been marked as a CA certificate by using basicConstraints with the CA flag set to True (and implicitly tests that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation). For each of the following tests the evaluator shall create a chain of at least three certificates: - a self-signed root CA certificate, - an intermediate CA certificate and - a leaf (node) certificate. The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain). Test 1: The evaluator shall ensure that at least one of the CAs in the chain does not contain the basicConstraints extension. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: *(i) as part of the validation of the leaf certificate belonging to this chain;* *(ii) (ii) when attempting to add a CA certificate without the basicConstraints extension to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).*
Test Steps	• Create a CA certificate that does not contain the basic Constraints extension. • Load the CA and local certificate onto the TOE. • Verify that the TOE identifies the signing CA certificate does not contain the basic Constraints extension rejects the certificate signed by it via TOE logs.
Expected Test Results	The TOE rejects improper certificates
Pass/Fail with Explanation	Pass. The TOE does not accept certificates that do not have the correct parameters as a CA certificate.

5.78 FIA_X509_EXT.1.2/Rev Test #2

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) then the associated extendedKeyUsage rule testing may be omitted. The goal of the following tests it to verify that the TOE accepts only certificates that have been marked as CA certificates by using basicConstraints with the CA flag set to True (and implicitly that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation). For each of the following tests the evaluator shall create a chain of at least three certificates: - a self-signed root CA certificate, - an intermediate CA certificate and - a leaf (node) certificate. The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain). Test 2: The evaluator shall ensure that at least one of the CA certificates in the chain has a basicConstraints extension in which the CA flag is set to FALSE. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: 1. As part of the validation of the leaf certificate belonging to this chain; 2. When attempting to add a CA certificate with the CA flag set to FALSE to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).
Test Steps	• Create a CA certificate that has the CA flag in the basicConstraints extension set to FALSE. • Load the CA and local certificate unto the TOE and verify that the TOE rejects the certificate via TOE logs.
Expected Test Results	The TOE will only accept a certificate if it has been makes as a CA certificate by using basicConstraints with the CA flag set to True.
Pass/Fail with Explanation	Pass. The TOE will only accept a certificate if it has been makes as a CA certificate by using basicConstraints with the CA flag set to True.

5.79 FIA_X509_EXT.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following test for each trusted channel: The evaluator shall demonstrate that using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate and observe that the action selected in FIA_X509_EXT.2.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the guidance documentation to determine that all supported administrator-configurable options behave in their documented manner.
Test Steps	• Delete the CRL from the repository and verify that the TOE can no longer fetch a new CRL. • Verify that the TOE does not establish a connection when it cannot fetch a CRL using TOE logs. • Verify the connection between TOE and peer fails using packet capture.

Expected Test Results	The TOE rejects the connection when it cannot verify the validity of any part of the trust chain.
Pass/Fail with Explanation	Pass; the TOE correctly rejected the certificate when it would not verify the validity of the trust chain.

5.80 FIA_X509_EXT.3 Test #1

Item	Data
Test Assurance Activity	The evaluator shall use the guidance documentation to cause the TOE to generate a Certification Request. The evaluator shall capture the generated message and ensure that it conforms to the format specified. The evaluator shall confirm that the Certification Request provides the public key and other required information, including any necessary user-input information.

Test Steps	• From the TOE, generate a CSR.
	• Examine the CSR contents to ensure the CSR contains the following fields:
	  ○ Public key
	  ○ Common Name
	  ○ Organization
	  ○ Country

Expected Test Results	The TOE generates a properly formatted CSR
Pass/Fail with Explanation	Pass; the TOE generated a properly formatted CSR

5.81 FIA_X509_EXT.3 Test #2

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that validating a response message to a Certification Request without a valid certification path results in the function failing. The evaluator shall then load a certificate or certificates as trusted CAs needed to validate the certificate response message and demonstrate that the function succeeds.
Test Steps	• From the TOE, generate a CSR request and generate a signed certificate based on the generated CSR from an external CA. • Ensure that the full trust chain for the signed CA is not present on the TOE. • Load the signed certificate on the TOE and verify that the TOE rejects the certificate because the full trust chain of the CA is not present. • Add the intermediary certificates to the TOE certificate store to ensure that the signing CA now has a full certificate path. • Re-attempt to load the signed certificate on the TOE verify that the TOE accepts the certificate because the path validation succeeded.
Expected Test Results	The TOE generates a CSR, and can import a correct certificate chain when the certificates are installed in the correct trust order.
Pass/Fail with Explanation	Pass; the TOE accepted the certificate chain when they were installed in the correct order.

5.82 FCS_IPSEC_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting a packet, and allowing a packet to flow in plaintext. The selectors used in the construction of the rule shall be different such that the evaluator can generate a packet and send packets to the gateway with the appropriate fields (fields that are used by the rule - e.g., the IP addresses, TCP/UDP ports) in the packet header. The evaluator performs both positive and negative test cases for each type of rule (e.g. a packet that matches the rule and another that does not match the rule). The evaluator observes via the audit trail, and packet captures that the TOE exhibited the expected behavior: appropriate packets were dropped, allowed to flow without modification, encrypted by the IPsec implementation.
Test Steps	All off the following cases will use the same SPD, consisting of • IPsec tunnel mode between 4.0.0.0/30 and 1.0.0.0/30 • FORWARD traffic accepted between 4.0.0.0/30 and 1.0.0.0/30 • FORWARD traffic accepted to or from 4.0.0.4 • INPUT traffic accepted from 4.0.0.4 • OUTPUT traffic accepted to 4.0.0.4 • INPUT traffic dropped from 4.0.0.3 ALLOW POSITIVE TEST • Configure IKE/IPsec rules on the TOE to Allow (PROTECT) a specific type of traffic. • Send traffic that will be protected (ping from 4.0.0.1 to 1.0.0.1) • Capture the traffic flows to and from the device. • Verify that the traffic is processed as required for the configured IKEv2/IPsec rules. NEGATIVE TEST • Send traffic that does not match the configured rules. (ping from 4.0.0.1 to 2.0.0.1) • Verify that there were no specific logs generated related to matching rules. • Verify that the packets were unencrypted via packet capture. DENY POSITIVE TEST • Configure IKE/IPsec rules on the TOE to DENY a specific type of traffic. • Send traffic that will be denied (ping from 4.0.0.3 to 2.0.0.1) • Capture the traffic flows to and from the device. • Verify that the traffic is processed as required for the configured IKEv2/IPsec rules. NEGATIVE TEST • Send traffic that does not match the configured rules and hits another rule (ping from 4.0.0.4 to 2.0.0.1) • Verify the same via logs. • Verify that the packets were allowed via the packet capture. BYPASS POSITIVE TEST • Configure IKE/IPsec rules on the TOE to send plaintext (BYPASS) a specific type of traffic. • Send traffic that will match the bypass rule (ping from 4.0.0.4 to 1.0.0.4) • Capture the traffic flows to and from the device.

	• Verify that the traffic is processed as required for the configured IKEv2/IPsec rules. NEGATIVE TEST • Send traffic that does not match the configured rules. (ping from 4.0.0.3 to 1.0.0.4) • Verify that there were no specific logs generated related to matching rules. • Verify that the packets were not bypassed via packet capture.
Expected Test Results	• The TOE should be able to implement rules for dropping a packet, encrypting a packet, and allowing a packet to flow in plaintext. • Evidence (screenshot or CLI output) of configuring the SPD. • Packet capture of each traffic flow.
Pass/Fail with Explanation	**PASS** **In each case, traffic was handled as expected according to the SPD. Packet captures show when traffic is encrypted and when it isn't.**

5.83 FCS_IPSEC_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall devise several tests that cover a variety of scenarios for packet processing. As with Test 1, the evaluator ensures both positive and negative test cases are constructed. These scenarios must exercise the range of possibilities for SPD entries and processing modes as outlined in the TSS and guidance documentation. Potential areas to cover include rules with overlapping ranges and conflicting entries, inbound and outbound packets, and packets that establish SAs as well as packets that belong to established SAs. The evaluator shall verify, via the audit trail and packet captures, for each scenario that the expected behavior is exhibited, and is consistent with both the TSS and the guidance documentation.
Test Steps	**Configuration 1**: Rules for a small, encrypted address range overlapping with larger plaintext range. Additionally includes conflict with a rule to drop a specific packet within the larger plaintext subnet rule. • ALLOW from src 1.0.0.0/24 dest 4.0.0.0/24 • ALLOW from src 4.0.0.0/24 dest 1.0.0.0/24 • ENCRYPT between src 1.0.0.0/30 and 4.0.0.0/30 • DROP from src 4.0.0.5/32 to dest any on INPUT and FORWARD **Test 1:** Using configuration 1, perform the following tests and verify expected behavior via packet captures and ToE logs. • Ping from 4.0.0.1 to 1.0.0.1 (verify encryption) • Ping from 4.0.0.4 to 1.0.0.4 (verify plaintext) • Ping from 4.0.0.5 to 1.0.0.4 (verify dropped) • Ping from 4.0.0.5 to 10.0.26.41.1 (verify failure) • Ping from 4.0.0.9 to 10.0.41.1 (verify success) **Configuration 2**: Rules for a large encrypted subnet to subnet, with an overlapping range to DENY. • ENCRYPT between 1.0.0.0/24 and 4.0.0.0/24 • DROP from src 4.0.0.0/30 dest 1.0.0.0/30

	Test 2: Using configuration 2, perform the following tests and verify expected behavior via packet captures and ToE logs. • Ping from 4.0.0.4 to 1.0.0.4 (verify encryption) • Ping from 4.0.0.1 to 1.0.0.2 (verify dropped) • Ping from 4.0.0.1 to 1.0.0.4 (verify dropped) • Ping from 4.0.0.6 to 1.0.0.9 (verify encryption) • Ping from 10.0.1.1 to 10.0.41.1 (verify plaintext) **Configuration 3**: Rules for denying all forwarding traffic and only allowing access to one address via the INPUT chain, and one single source and destination overlap for forwarding. • DROP on FORWARD for all traffic • ALLOW from src 10.0.41.1 to 10.1.1.1 on OUTPUT • ALLOW from 10.1.1.1 to 10.0.41.1 on INPUT • ALLOW from 4.0.0.9/32 to 1.0.0.2/32 on FORWARD **Test 1:** Using configuration 3, perform the following tests and verify expected behavior via packet captures and ToE logs. • Ping from 4.0.0.5 to 1.0.0.3 (verify dropped) • Ping from 4.0.0.2 to 1.0.0.9 (verify dropped) • Ping from 4.0.0.9 to 1.0.0.2 (verify success)
Expected Test Results	For each case described above, the expected result of the attempt to pass ICMP packets across the network should be observed either through packet captures or through logs generated by the ToE.
Pass/Fail with Explanation	**Pass.** For all 3 configurations, the packets are either dropped, passed, or encrypted by the ToE as expected by the SPD configurations. The tests verified that even with overlapping rules, the packets are processed in the order expected as programmed into the SPD.

5.84 FCS_IPSEC_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting a packet, and allowing a packet to flow in plaintext. The evaluator may use the SPD that was created for verification of FCS_IPSEC_EXT.1.1. The evaluator shall construct a network packet that matches the rule to allow the packet to flow in plaintext and send that packet. The evaluator should observe that the network packet is passed to the proper destination interface with no modification. The evaluator shall then modify a field in the packet header; such that it no longer matches the evaluator-created entries (there may be a "TOE created" final entry that discards packets that do not match any previous entries). The evaluator sends the packet and observes that the packet was dropped.
Test Steps	The following steps will be carried out using the same SPD as 1.1 #1, consisting of the following: • IPsec tunnel mode between 4.0.0.0/30 and 1.0.0.0/30 • FORWARD traffic accepted between 4.0.0.0/30 and 1.0.0.0/30

	• FORWARD traffic accepted to or from 4.0.0.4 • INPUT traffic accepted from 4.0.0.4 • OUTPUT traffic accepted to 4.0.0.4 • INPUT traffic dropped from 4.0.0.3 In addition, when the SPD has been set up, the iptables ruleset will be examined to confirm that the system provides default drop rules that did not have to be added by the tester. • Configure policy on TOE to allow the packet to flow in plaintext. • Attempt a connection between 4.0.0.4 and 1.0.0.4 • Verify connection is successful. • Verify the packet capture. • Attempt a connection with modified header. (4.0.0.3 to 4.0.0.1) • Verify connection is unsuccessful. • Verify the packet capture.
Expected Test Results	• The TOE provides default drop rules as the last rules in the chain • For each case described above, the expected result of the attempt to pass ICMP packets across the network should be observed either through packet captures or through logs generated by the ToE.
Pass/Fail with Explanation	**PASS** • The TOE was configured with default drop rules. • Traffic passed through unencrypted in the positive case and did not in the negative case.

5.85 FCS_IPSEC_EXT.1.3 Test #1

Item	Data
Test Assurance Activity	If **tunnel mode** is selected, the evaluator uses the guidance documentation to configure the TOE to operate in tunnel mode and also configures a VPN peer to operate in tunnel mode. The evaluator configures the TOE and the VPN peer to use any of the allowable cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator shall then initiate a connection from the TOE to connect to the VPN peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the tunnel mode.
Test Steps	• Configure an IKEv2/IPsec connection (ensure that tunnel mode is configured). • Initiate traffic through IPsec Tunnel. • Verify Tunnel mode was used with logs. • Verify with packet capture.
Expected Test Results	• TOE is configured in tunnel mode • Traffic passes through tunnel successfully • Logs and packet capture show encryption of the traffic
Pass/Fail with Explanation	PASS • TOE configured to use tunnel mode per iked.conf • Logs show tunnel establishment • Pcap shows IKE exchange and encrypted traffic

5.86 FCS_IPSEC_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure the TOE as indicated in the guidance documentation configuring the TOE to use each of the supported algorithms, attempt to establish a connection using ESP, and verify that the attempt succeeds.
Test Steps	• Configure the TOE for IKEv2 AES-CBC-256 & HMAC-SHA-384 configuration in the ESP. • Configure the PEER for IKEv2 AES-CBC-256 & HMAC-SHA-384 configuration in ESP. • Start an IPsec connection (using Ping). • Verify via logs that the connection was established using AES-CBC-256 & HMAC-SHA-384. • Verify via packet capture that the connection was established using AES-CBC-256 & HMAC-SHA-384.
Expected Test Results	The ipsec tunnel between the TOE and the peer is encrypted using the required algorithms.
Pass/Fail with Explanation	PASS The TOE successfully established a tunnel using AES-256-CBC and HMAC-SHA-384 algorithms

5.87 FCS_IPSEC_EXT.1.6 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure the TOE to use the ciphersuite under test to encrypt the IKEv1 and/or IKEv2 payload and establish a connection with a peer device, which is configured to only accept the payload encrypted using the indicated ciphersuite. The evaluator will confirm the algorithm was that used in the negotiation.
Test Steps	• Configure the TOE with an IKEv2 policy using AES-CBC-256. • Configure the Peer with an IKEv2 policy using AES-CBC-256. • Attempt a connection between the two devices. • Verify that the negotiation uses AES-CBC-256 as specified in the policy using TOE logs. • Verify that the negotiation uses AES-CBC-256 as specified in the policy using packet capture.
Expected Test Results	The ipsec tunnel between the TOE and the peer is encrypted using the required algorithms.
Pass/Fail with Explanation	PASS The IKEv2 exchange to establish the ESP SA was encrypted using the required algorithms.

5.88 FCS_IPSEC_EXT.1.7 Test #2

Item	Data
Test Assurance Activity	Test 2: If 'length of time' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime no later than 24 hours for the Phase 1 SA following the guidance documentation. The evaluator shall configure a test peer with a Phase 1 SA lifetime that exceeds the Phase 1 SA lifetime on the TOE. **TD 0633 applied.**

Test Steps	• Configure the IKE SA Lifetime more than 73800 seconds on the TOE. • Configure the IKE SA Lifetime for 24 hours on the peer. • Establish and maintain an IPsec connection between the TOE and peer for 24 hours. • Verify that a rekey was initiated before 24 hours via log review.
Expected Test Results	The TOE will renegotiate a rekey before the 24 hours is up, which will be verified by TOE logs
Pass/Fail with Explanation	PASS TOE successfully renegotiates the IKE session.

5.89 FCS_IPSEC_EXT.1.8 Test #1

Item	Data
Test Assurance Activity	Test 1: If '**number of bytes**' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime in terms of the number of bytes allowed following the guidance documentation. The evaluator shall configure a test peer with a byte lifetime that exceeds the lifetime of the TOE. The evaluator shall establish a SA between the TOE and the test peer, and determine that once the allowed number of bytes through this SA is exceeded, a new SA is negotiated. The evaluator shall verify that the TOE initiates a Phase 2 negotiation.
Test Steps	• Configure the bytes per lifetime. • Establish an IPsec session. • Transmit packets across the connections repeatedly. • Verify that a rekey was initiated when the bytes threshold is crossed via TOE logs and packet capture.
Pass/Fail with Explanation	PASS The TOE establishes a tunnel and sends several encrypted messages before renegotiating the child SA.

5.90 FCS_IPSEC_EXT.1.8 Test #2

Item	Data
Test Assurance Activity	Test 2: If 'length of time' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime no later than 8 hours for the Phase 2 SA following the guidance documentation. The evaluator shall configure a test peer with a Phase 2 SA lifetime that exceeds the Phase 2 SA lifetime on the TOE. **TD 0633 applied.**
Test Steps	• Configure the Phase 2 SA Lifetime as 8 hours (28800 seconds) on the TOE • Configure the Phase 2 SA for more than 8 hours (30000 seconds) on the peer • Establish and maintain an IPsec connection between the TOE and peer for 8 hours. • Verify that a rekey was initiated before 8 hours via log review and packet capture.
Expected Test Results	The ipsec sa is rekeyed after the tunnel is established and the time has elapsed.

Pass/Fail with Explanation	PASS The TOE successfully rekeys the ipsec SA for time expiration.

5.91 FCS_IPSEC_EXT.1.11 Test #1

Item	Data
Test Assurance Activity	For each supported DH group, the evaluator shall test to ensure that all supported IKE protocols can be successfully completed using that particular DH group.
Test Steps	• Configure DH group 20 for IKEv2 on TOE. • Configure DH group 20 for IKEv2 on PEER. • Start an IPsec connection (using Ping). • Verify that DH Group 20 was used via log. • Verify that Group 20 is used via capture.
Expected Test Results	The tunnel is successfully established with Diffie hellman group 20.
Pass/Fail with Explanation	PASS The TOE is using the configured Diffie hellman group (20) to negotiate the tunnel.

5.92 FCS_IPSEC_EXT.1.12 Test #1

Item	Data
Test Assurance Activity	This test shall be performed for each version of IKE supported. The evaluator shall successfully negotiate an IPsec connection using each of the supported algorithms and hash functions identified in the requirements.
Pass/Fail with Explanation	Pass. This testing is covered by the requirements in FCS_IPSEC_EXT.1.4 Test#1 and FCS_IPSEC_EXT.1.6 Test#1.

5.93 FCS_IPSEC_EXT.1.12 Test #2

Item	Data
Test Assurance Activity	This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish a SA for ESP that selects an encryption algorithm with more strength than that being used for the IKE SA (i.e., symmetric algorithm with a key size larger than that being used for the IKE SA). Such attempts should fail.
Test Steps	• Configure TOE to use AES-CBC-256 in P1 and AES-CBC-256 in P2 IKEv2. • Configure peer to use AES-CBC-256 in P1 and AES-CBC-128 in P2 IKEv2. • Attempt to establish a connection. • Verify the connection is rejected using logs. • Verify the connection is rejected using Packet Capture.
Expected Test Results	TOE logs and packet capture show rejection of the tunnel due to insufficient algorithm strength
Pass/Fail with	PASS

Explanation	The logs and pcap show the TOE failing to negotiate a tunnel due to algorithm complaints.

5.94 FCS_IPSEC_EXT.1.12 Test #3

Item	Data
Test Assurance Activity	This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an IKE SA using an algorithm that is not one of the supported algorithms and hash functions identified in the requirements. Such an attempt should fail.
Test Steps	• Configure the TOE to use AES and SHA-256. • Configure the Peer to use 3DES and SHA-256. • Attempt a secure IPsec connection from peer. • Verify the logs reflected on the TOE. • Verify the connection is rejected via packet capture.
Expected Test Results	TOE rejects the connection and the logs show that the algorithm proposal was not sufficient.
Pass/Fail with Explanation	PASS TOE fails to negotiate proposal and complains about peer algorithm.

5.95 FCS_IPSEC_EXT.1.12 Test #4

Item	Data
Test Assurance Activity	This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish a SA for ESP (assumes the proper parameters where used to establish the IKE SA) that selects an encryption algorithm that is not identified in FCS_IPSEC_EXT.1.4. Such an attempt should fail.

Test Steps	• Configure the TOE to support the following algorithms:
	  • IKE SA (Phase 1): AES-CBC-256, HMAC-SHA-384
	  • IPsec SA (Phase 2): AES-CBC-256, HMAC-SHA-384
	• Configure a peer to support the following algorithms:
	  • IKE SA (Phase 1): AES-CBC-128, SHA-256
	  • IPsec SA (Phase 2): Triple-DES, SHA-256
	• Attempt to make a connection.
	• Verify that the connection cannot be established via logs.
	• Verify that the connection cannot be established via packet Capture.

Expected Test Results	TOE rejects ipsec SA based on algorithm proposal.
Pass/Fail with Explanation	PASS ESP SA was not successfully negotiated because 3des is not acceptable.

5.96 FCS_IPSEC_EXT.1.14 Test #2

Item	Data
Test Assurance Activity	Test 2: [conditional] For each SAN/identifier type combination selected, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the field in the peer's presented certificate and shall verify that the IKE

	authentication succeeds. If the TOE prioritizes SAN checking over CN (through explicit specification of the field when specifying the reference identifier or prioritization rules), the evaluator shall also configure the CN so it contains an incorrect identifier formatted to be the same type (e.g. the reference identifier on the TOE is DNS-ID; identify certificate has an identifier in SAN with correct DNS-ID, CN with incorrect DNS-ID (and not a different type of identifier)) and verify that IKE authentication succeeds.
Test Steps	• Create and load a peer certificate with a correct FQDN in the SAN but an incorrect FQDN in the CN field. • Configure the correct FQDN on the TOE's peer reference identifier. • Verify through logs and a packet capture that the connection succeeds.
Pass/Fail with Explanation	PASS Tunnel established successfully.

5.97 FCS_IPSEC_EXT.1.14 Test #4

Item	Data
Test Assurance Activity	Test 4: [conditional] For each SAN/identifier type combination selected, the evaluator shall: a) Create a valid certificate with an incorrect identifier in the SAN. The evaluator shall configure a string representation of the correct identifier in the DN. If the TOE prioritizes CN checking over SAN (through explicit specification of the field when specifying the reference identifier or prioritization rules) for the same identifier type, the addition/modification shall be to any non-CN field of the DN. Otherwise, the addition/modification shall be to the CN. b) Configure the peer's reference identifier on the TOE (per the administrative guidance) to match the correct identifier (expected in the SAN) and verify that IKE authentication fails.
Test Steps	• Create and load a peer certificate with an incorrect FQDN in the SAN but a correct FQDN in the CN field. • Configure the correct FQDN on the TOE's peer reference identifier. • Verify through logs and a packet capture that the connection fails.
Pass/Fail with Explanation	PASS TOE did not establish tunnel when SAN was incorrect.

5.98 FCS_IPSEC_EXT.1.14 Test #5

Item	Data
Test Assurance Activity	Test 5: [conditional] If the TOE supports DN identifier types, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the subject DN in the peer's presented certificate and shall verify that the IKE authentication succeeds.
Test Steps	• Configure a peer certificate with DN identifier types countryName, organizationalName, commonName

	• Configure the TOE to use DN as the peer identity. • Verify that the connection succeeds.
Expected Test Results	TOE is able to establish tunnel using DN as peer identity.
Pass/Fail with Explanation	PASS TOE was able to establish a tunnel while matching on DN.

5.99 FCS_IPSEC_EXT.1.14 Test #6a

Item	Data
Test Assurance Activity	Test 6: [conditional] If the TOE supports **DN** identifier types, to demonstrate a bit-wise comparison of the DN, the evaluator shall create the following valid certificates and verify that the IKE authentication fails when each certificate is presented to the TOE: a) Duplicate the CN field, so the otherwise authorized DN contains two identical CNs.
Test Steps	• Create a peer certificate with a single CN field. • Use a hex editor to duplicate CN on the DN of the certificate. • Present this certificate to the TOE and verify that the IKE authentication fails. • Verify the failure via logs and/or packet capture.
Expected Test Results	TOE should reject IKE authentication because the DN has too many CN fields. No tunnel should be established. This should be reflected in logs or packet captures.
Pass/Fail with Explanation	PASS Logs show TOE rejected negotiation

5.100 FCS_IPSEC_EXT.1.14 Test #6b

Item	Data
Test Assurance Activity	Test 6: If the TOE supports **DN** identifier types, to demonstrate a bit-wise comparison of the DN, the evaluator shall create the following valid certificates and verify that the IKE authentication fails when each certificate is presented to the TOE: b) Append '\0' to a non-CN field of an otherwise authorized DN.
Test Steps	• Create a peer certificate with '\0' appended to non-CN field. • Present this certificate to the TOE and verify that the IKE authentication fails. • Verify the failure via packet capture.
Expected Test Results	TOE rejects the negotiation for the tunnel because the Organization identifier of the DN has a \0 appended to it
Pass/Fail with Explanation	PASS The TOE logs show the negotiation failed because the DN did not match what was expected.

5.101 FPT_TST_EXT.1 Test #1

Item	Data
Test Assurance Activity	It shall be expected that at least the following tests are performed:

	a) Verification of the integrity of the firmware and executable software of the TOE b) Verification of the correct operation of the cryptographic functions necessary to fulfil any of the SFRs. The evaluator shall either verify that the self-tests described above are carried out during initial start-up or that the developer has justified any deviation from this. For distributed TOEs the evaluator shall perform testing of self-tests on all TOE components according to the description in the TSS about which self-test are performed by which component.
Test Steps	Part A 1. Follow the guidance documentation to enable updates. 2. Load a new update package into a TFTP directory connected to the ToE 3. Reboot the ToE and observe the console logs to see verification of the firmware and the software image. Part B 1. Update the ToE according to the guidance documentation. 2. Verify kernel self-tests passed by searching **/proc/crypto** for evidence the self-tests ran. 3. Verify boringssl in FIPS mode by checking strings in the binary
Expected Test Results	Part A - Observe validation of firmware image with RSA 4096 keys and SHA2-384 in the first stage bootloader on startup - Observe validation of the software image with SHA-2 384 by U-Boot on startup Part B - Observe log message confirming Kernel self-tests passed. - Confirm the crypto library binary has been compiled in FIPS mode and show self-tests included. - No test for SE050F. This hardware component is FIPS validated and performs required self-tests on startup.
Pass/Fail with Explanation	**Pass.** Firmware validation with RSA and software validation with SHA2-384 was observed in the serial console after reboot. Self-testing on startup is performed, confirmed either with direct logs or indirectly by confirming FIPS certifications for components performing cryptographic functions.

5.102 FPT_TUD_EXT.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the version verification activity to determine the current version of the product as well as the most recently installed version (should be the same version before updating). The evaluator obtains a legitimate update using procedures described in the guidance documentation and verifies that it is successfully installed on the TOE. (For some TOEs loading the update onto the TOE and activation of the update are separate steps ('activation' could be performed e.g. by a distinct activation step or by rebooting the device). In that case the evaluator verifies after loading the update onto the TOE but before activation of the update that the current version of the product did

	not change but the most recently installed version has changed to the new product version.) After the update, the evaluator performs the version verification activity again to verify the version correctly corresponds to that of the update and that current version of the product and most recently installed version match again.
Test Steps	1. Log into the ToE and run the **version_info** command. 2. Follow the guidance documentation to enable updates 3. Load a new update package into a TFTP directory connected to the ToE 4. Reboot the device
Expected Test Results	Observe a change in Platform Version and Kernel Version after reboot by performing version verification with the supported version_info command before and after an update performed according to the guidance documentation.
Pass/Fail with Explanation	**Pass.** The relevant fields in the ToE's reported version information successfully changed after following the update guidance, both for firmware (Platform Version) and software (Kernel Version).

5.103 FPT_TUD_EXT.1 Test #2 (a)

Item	Data
Test Assurance Activity	Test 2 [conditional]: If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed (otherwise the test shall be omitted). The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates: 1) A modified version (e.g. using a hex editor) of a legitimately signed update
Test Steps	Verify Image.fit.ecc software checking with SHA2-384 1. Modify a software update **Image.fit.ecc** by 1 byte using a hex editor 2. Load the modified **Image.fit.ecc** into the TFTP server to transfer the logs to the device on reboot. 3. Enable updates on the ToE. 4. Reboot to trigger the update process. Observe on the serial console the rejection of the software update Image. 5. Update the ToE to the previous good version. Verify boot.bin firmware RSA 4096 signature verification. 1. Modify a **boot.bin** by 1 byte using a hex editor 2. Load the modified **boot.bin** into the TFTP server to transfer the logs to the device on reboot. 3. Enable updates on the ToE. • Reboot to trigger the update process. Observe on the serial console the rejection of the firmware update Image.
Expected Test Results	Observe a failure to match the hash of the Image.fit.ecc while software integrity checking is being performed. The device fails to boot the updated image. Observe a failure to validate the RSA signature on the firmware (U-Boot) in the serial console on

	update. The device fails to boot the updated image.
Pass/Fail with Explanation	**Pass.** The Image.fit.ecc fails the software integrity check while attempting to update to the corrupted image. The mismatching hashes are displayed in the console boot logs. The device fails to boot the updated image. The firmware (U-Boot) image fails the software integrity check while attempting to update to the corrupted image. The mismatching hashes are displayed in the serial console on update. The device fails to boot, showing that if either part of the boot chain is compromised (software or firmware), the device will refuse to update.

5.104 FPT_TUD_EXT.1 Test #2 (b)

Item	Data
Test Assurance Activity	[conditional]: If **the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE** the following test shall be performed (otherwise the test shall be omitted). The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates: 2) An image that has not been signed
Test Steps	1. Generate a **boot.bin** image that does not contain the RSA signature required to validate U-Boot. 2. Load the modified **boot.bin** into the TFTP server to transfer the logs to the device on reboot. 3. Enable updates on the ToE. 4. Reboot to trigger the update process. Observe on the serial console the rejection of the firmware update Image. 5. After boot, show that the version of the combined firmware and software has not changed by checking Platform Version and Kernel Version
Expected Test Results	Observe a failure to validate the RSA signature on the firmware image. Observe no change to the version information displayed on the ToE after the attempted update.
Pass/Fail with Explanation	**Pass.** The firmware (U-Boot) image fails the software integrity check while attempting to update with an image missing an expected signature. The mismatching hashes are displayed in the serial console on update.

5.105 FPT_TUD_EXT.1 Test #2 (c)

Item	Data
Test Assurance Activity	[conditional]: If **the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE** the following test shall be performed (otherwise the test shall be omitted). The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces

	illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates: 3) An image signed with an invalid signature (e.g. by using a different key as expected for creating the signature or by manual modification of a legitimate signature)
Test Steps	Generate a boot.bin image that has been signed by a different RSA key than the one burned into fuses on the device as "trusted". Load the modified boot.bin into the TFTP server to transfer the logs to the device on reboot. Enable updates on the ToE. Reboot to trigger the update process. Observe on the serial console the rejection of the firmware update Image. After boot, show that the version of the combined firmware and software has not changed
Expected Test Results	Observe a failure to validate the RSA signature on the firmware image. Observe no change to the version information displayed on the ToE after the attempted update.
Pass/Fail with Explanation	Pass. The firmware (U-Boot) image fails the software integrity check while attempting to update with an image missing an expected signature. The mismatching hashes are displayed in the serial console on update.

6 Security Assurance Requirements

6.1 ADV_FSP.1 Basic Functional Specification

6.1.1 ADV_FSP.1

6.1.1.1 ADV_FSP.1 Activity 1

Objective	The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to verify that it describes the purpose and method of use for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the purpose and method of use for each security relevant TSFI by verifying the AGD satisfies all of the Guidance Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.1.1.2 ADV_FSP.1 Activity 2

Objective	The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to develop a mapping of the interfaces to SFRs. The evaluator examined the entire AGD. Each Guidance Evaluation Activity is associated with a specific SFR. The Evaluation Findings for each Guidance Evaluation Activity identify the relevant interfaces, thus providing a mapping. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.1.1.3 ADV_FSP.1 Activity 3

Objective	The evaluator shall check the interface documentation to ensure it identifies and describes the parameters for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to verify that it identifies and describes the parameters for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the parameters for each security relevant TSFI by verifying the AGD satisfies all of the Guidance Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.2 AGD_OPE.1 Operational User Guidance

6.2.1 AGD_OPE.1

6.2.1.1 AGD_OPE.1 Activity 1

Objective	The evaluator shall ensure the Operational guidance documentation is distributed to Security Administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that Security Administrators and users are aware of the existence and role of the

	documentation in establishing and maintaining the evaluated configuration.
Evaluator Findings	The evaluator checked the requirements below are met by the guidance documentation. Guidance documentation shall be distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration. Upon investigation, the evaluator found that the CC guidance will be published with the CC certificate on www.niap-ccevs.org.. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.2.1.2 AGD_OPE.1 Activity 2

Objective	The evaluator shall ensure that the Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target.
Evaluator Findings	The evaluator ensured that the Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target. The section titled Supported Platforms of the AGD was used to determine the verdict of this assurance activity. The AGD specifies that the platforms supported are: The physical boundary of the TOE is the SpaceX Regulus chassis, which is a networked device providing connectivity to external networked entities. The TOE includes a specialized PCB board containing a Zynq Ultrascale+ ZU5 System on Chip (SoC) processor, based on Armv8-A Architecture, which executes the TOE software along with a NXP SE050F cryptographic accelerator. The TOE provides the following interfaces for management and network connectivity: • 1x 100Mbps and 1x 10Gbps Ethernet ports for connectivity to trusted networks • 1x 100Mbps, 1x 1Gbps, and 1x 10Gbps Ethernet ports for connectivity to untrusted networks • UART for local serial console access • 120VAC power input Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.2.1.3 AGD_OPE.1 Activity 3

Objective	The evaluator shall ensure that the Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.
Evaluator Findings	The evaluator ensured that the Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. While performing the Guidance Evaluation Activities for the cryptographic SFRs, the evaluator ensured guidance contained the necessary instructions for configuring the cryptographic engines. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.2.1.4 AGD_OPE.1 Activity 4

Objective	The evaluator shall ensure the Operational guidance makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs.
Evaluator Findings	The entire AGD was used to determine the verdict of this work unit. Each confirmation command indicates tested options. Additionally, the section titled XXXX specifies features that are not assessed and tested by the EAs. The evaluator ensured the Operational guidance makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.2.1.5 AGD_OPE.1 Activity 5 **[TD0536]**

Objective	In addition, the evaluator shall ensure that the following requirements are also met. a) The guidance documentation shall contain instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE. b) The documentation must describe the process for verifying updates to the TOE for each method selected for FPT_TUD_EXT.1.3 in the Security Target. The evaluator shall verify that this process includes the following steps: i) Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory). ii) Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes instructions that describe at least one method of validating the hash/digital signature. c) The TOE will likely contain security functionality that does not fall in the scope of evaluation under this cPP. The guidance documentation shall make it clear to an administrator which security functionality is covered by the Evaluation Activities.
Evaluator Findings	The evaluator verified the guidance documentation contains instructions for configuring any cryptographic engines in AGD_OPE.1 Test #3. The evaluator verified the guidance documentation describes the process for verifying updates in FPT_TUD_EXT.1 Guidance 2. The evaluator verified the guidance documentation makes it clear which security functionality is covered by the Evaluation Activities in AGD_OPE.1 Test #4. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.3 AGD_PRE.1 Preparative Procedures

6.3.1 AGD_PRE.1

6.3.1.1 AGD_PRE.1 Activity 1

Objective	The evaluator shall examine the Preparative procedures to ensure they include a description of how the Security Administrator verifies that the operational environment can fulfil its role to support the security functionality (including the requirements of the Security Objectives for the Operational

<table>
<tr><td></td><td>Environment specified in the Security Target).</td></tr>
<tr><td>Evaluator Findings</td><td>The evaluator examined the Preparative procedures to ensure they include a description of how the administrator verifies that the operational environment can fulfil its role to support the security functionality. The evaluator reviewed the sections titled XXXX of the AGD. The evaluator found that these sections describe how the Operational Environment must meet:

The following environmental components are required to operate the TOE in the evaluated configuration:
Table 1 – Required Environmental Components<table><tr><th>Component</th><th>Purpose/Description</th></tr><tr><td>VPN Peer</td><td>Peer VPN endpoint and audit log receiver</td></tr><tr><td>Management PC</td><td>Local/remote management and TFTP service for firmware updates</td></tr></table>
Based on these findings, this assurance activity is considered satisfied.</td></tr>
<tr><td>Verdict</td><td>Pass</td></tr>
</table>

6.3.1.2 AGD_PRE.1 Activity 2

<table>
<tr><td>Objective</td><td>The evaluator shall examine the Preparative procedures to ensure they are provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target.</td></tr>
<tr><td>Evaluator Findings</td><td>The evaluator checked the requirements below are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that the guidance documentation describes each of the devices in the operating environment, including,

The following environmental components are required to operate the TOE in the evaluated configuration:
Table 2 – Required Environmental Components<table><tr><th>Component</th><th>Purpose/Description</th></tr><tr><td>VPN Peer</td><td>Peer VPN endpoint and audit log receiver</td></tr><tr><td>Management PC</td><td>Local/remote management and TFTP service for firmware updates</td></tr></table>The section titled Secure Acceptance of the TOE of AGD identifies the following supported platform:

The physical boundary of the TOE is the SpaceX Regulus chassis, which is a networked device providing connectivity to external networked entities. The TOE includes a specialized PCB board containing a Zynq Ultrascale+ ZU5 System on Chip (SoC) processor, based on Armv8-A Architecture, which executes the TOE software along with a NXP SE050F cryptographic accelerator. The TOE provides the following interfaces for management and network connectivity:
• 1x 100Mbps and 1x 10Gbps Ethernet ports for connectivity to trusted networks
• 1x 100Mbps, 1x 1Gbps, and 1x 10Gbps Ethernet ports for connectivity to untrusted networks
• UART for local serial console access
• 120VAC power input

Based on these findings, this assurance activity is considered satisfied.</td></tr>
<tr><td>Verdict</td><td>Pass</td></tr>
</table>

6.3.1.3 AGD_PRE.1 Activity 3

Objective	The evaluator shall examine the preparative procedures to ensure they include instructions to successfully install the TSF in each Operational Environment.
Evaluator Findings	The evaluator checked the requirements are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that AGD describes all of the functions necessary to install and configure the TOE to work in the target operating environment, including, • Configuring Administrative Accounts and Passwords • Configuring SSH and Console Connections • Configuring the Remote Syslog Server • Configuring Audit Log Options • Configuring Event Logging • Configuring a Secure Logging Channel • Configuring VPNs (IPsec) • Configuring Security Flow Policies • Configuring Traffic Filtering Rules Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.3.1.4 AGD_PRE.1 Activity 4

Objective	The evaluator shall examine the preparative procedures to ensure they include instructions to manage the security of the TSF as a product and as a component of the larger operational environment.
Evaluator Findings	The evaluator ensured the preparative procedures include instructions to manage the security of the TSF as a product and as a component of the larger operational environment. The entire AGD was used to determine the verdict of this work unit. The same commands, configurations, and interfaces used to install the TOE are also used for ongoing management, so this is satisfied by AGD_PRE.1 Test #3. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.3.1.5 AGD_PRE.1 Activity 5

Objective	In addition, the evaluator shall ensure that the following requirements are also met. The preparative procedures must a) include instructions to provide a protected administrative capability; and b) identify TOE passwords that have default values associated with them and instructions shall be provided for how these can be changed.
Evaluator Findings	The evaluator ensured the preparative procedures include instructions to provide a protected administrative capability and changing default passwords. The sections titled Password Management were used to determine the verdict of this work unit. The AGD describes changing the default password associated with the root account and configuring SSH for remote administration.

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.4 ALC Assurance Activities

6.4.1 ALC_CMC.1

6.4.1.1 ALC_CMC.1 Activity 1

Objective	When evaluating that the TOE has been provided and is labelled with a unique reference, the evaluator performs the work units as presented in the CEM.
Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.4.2 ALC_CMS.1

6.4.2.1 ALC_CMS.1 Activity 1

Objective	When evaluating the developer's coverage of the TOE in their CM system, the evaluator performs the work units as presented in the CEM.
Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.5 ATE_IND.1 Independent Testing – Conformance

6.5.1 ATE_IND.1

6.5.1.1 ATE_IND.1 Activity 1

Objective	The evaluator performs the CEM work units associated with the ATE_IND.1 SAR. Specific testing requirements and EAs are captured for each SFR in Sections 2, 3 and 4. The evaluator should consult Appendix 709 when determining the appropriate strategy for testing multiple variations or models of the TOE that may be under evaluation.
Evaluator Findings	The evaluator examined the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST. Upon investigation, the evaluator found that each instance of the TOE used in testing was consistent with TOE description found in the Security Target. Additionally, the evaluator found that the TOE version is consistent with what was specified in the Security Target. The evaluator examined the TOE to determine that it has been installed properly and is in a known state. The details of the installed TOE and any configuration performed with the TOE are found in the separate Test Reports. The evaluator prepared a test plan that covers all of the testing actions for ATE_IND.1 in the CEM and in the SFR-related Evaluation Activities.

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.6 AVA_VAN.1 Vulnerability Survey

6.6.1 AVA_VAN.1

6.6.1.1 AVA_VAN.1 Activity 1 **[TD0564, Labgram #116]**

Objective	The evaluator shall document their analysis and testing of potential vulnerabilities with respect to this requirement.
Evaluator Findings	The evaluator documented their analysis and testing of potential vulnerabilities with respect to this requirement. Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The the evaluator examined sources of publicly available information to identify potential vulnerabilities in the TOE. The sources of examined are as follows: • https://nvd.nist.gov/view/vuln.search • http://cve.mitre.org/cve • https://www.cvedetails.com/vulnerability-search.php • https://www.kb.cert.org/vuls/search/ • www.exploitsearch.net • www.securiteam.com • http://nessus.org/plugins/index.php?view=search • http://www.zerodayinitiative.com/advisories • https://www.exploit-db.com • https://www.rapid7.com/db/vulnerabilities • https://www.spacex.com/ The evaluator performed the public domain vulnerability searches using the following key words. The search was performed on July 25, 2023. • SpaceX • Regulus • Zynq Ultrascale+ ZU5 • Linux-based Operating System based on Kernel 5.15 • OpenIKED version 7.1 • OpenSSH version 8.9 • BoringSSL version 5416e4f16 The evaluation lab examined each result provided from NVD and Exploit Search to determine if the current TOE version or component within the environment was vulnerable. Based upon the analysis, any issues found that were generated were patched in the TOE version and prior versions, mitigating the risk factor. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.6.1.2 AVA_VAN.1 Activity 2

Objective	The evaluator shall perform the following activities to generate type 4 flaw hypotheses: • Fuzz testing ○ Examine effects of sending: ▪ mutated packets carrying each 'Type' and 'Code' value that is undefined in the relevant RFC for each of ICMPv4 (RFC 792) and ICMPv6 (RFC 4443) ▪ mutated packets carrying each 'Transport Layer Protocol' value that is undefined in the respective RFC for IPv4 (RFC 791) IPv6 (RFC 2460) should also be covered if it is supported and claimed by the TOE. Since none of these packets will belong to an allowed session, the packets should not be processed by the TOE, and the TOE should not be adversely affected by this traffic. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis. ○ Mutation fuzz testing of the remaining fields in the required protocol headers. This testing requires sending mutations of well- formed packets that have both carefully chosen and random values inserted into each header field in turn (i.e. testing is to include both carefully chosen and random insertion test cases). The original well-formed packets would be accepted as part of a normal existing communication stream and may still be accepted as valid packets when subject to the carefully chosen mutations (the individual packet alone would be valid although its contents may not be valid in the context of preceding and/or following packets), but will often not be valid packets when random values are inserted into fields. The carefully chosen values should include semantically significant values that can be determined from the type of the data that the field represents, such as values indicating positive and negative integers, boundary conditions, invalid binary combinations (e.g. for flag sets with dependencies between bits), and missing start or end values. Randomly chosen values may not result in well-formed packets but are included nonetheless to see whether they can lead to the device entering an insecure state. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis.
Evaluator Findings	The evaluator documented the fuzz testing results with respect to this requirement. The evaluation lab examined each result from fuzz testing to determine if the TOE improperly processes packets. Based upon the analysis, no unexpected results occurred. Therefore, no Type 4 hypotheses were generated. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.6.1.3 AVA_VAN.1/VPN Activity 1

Objective	The evaluator shall perform the SAR Evaluation Activities defined in the NDcPP SD against the entire TOE (i.e., both the network device portion and the VPN gateway portion). In particular, the evaluator shall ensure that the vulnerability testing defined in section A.1.4 of the NDcPP SD is applied to the TOE's VPN interface(s) in addition to any other security-relevant network device interfaces that the TOE may have.
Evaluator Findings	The evaluation team performed a fuzzing test against the TOE to ensure only permitted, acceptable traffic would be able to pass through the interfaces protected by ACLs. The evaluation team documented this test and identified no issues with the product during

	execution of the test. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7 Conclusion

The testing shows that all test cases required for conformance have passed testing.

8 Appendix A – Certificate Table

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #	TSF Supported
FCS_CKM.1	ECC schemes using "NIST curves" [selection: P-256, P-384] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	SpaceX Cryptographic Module (BoringSSL)	ECDSA KeyGen	A3452	Public/Private key creation for X.509v3 Certificate CSRs. Peer authentication for IPsec Peer authentication for SSH
	FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526]	N/A	Vendor Affirmed	N/A	EC DH Key exchange for SSH EC DH Key exchange for IPsec
FCS_CKM.2	Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"	SpaceX Cryptographic Module (BoringSSL)	ECDSA Key Establishment	A3452	Ephemeral Key creation for IPsec Ephemeral Key creation for SSH
	FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [groups listed in RFC 3526]	N/A	Vendor Affirmed	N/A	EC DH Key exchange for SSH
FCS_COP.1/ DataEncryption	AES used in [CBC, GCM] mode and cryptographic key sizes [256 bits]	SpaceX Cryptographic Module (BoringSSL)	AES-CBC-256 AES-GCM-256	A3452	Bulk Encryption for IPsec Phase 1 SA's Bulk Encryption for SSH
		SpaceX Linux Kernel cryptographic Module	AES-CBC-256	A3121	Bulk Encryption for IPsec Phase 2 SA's.
FCS_COP.1/ SigGen	For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	SpaceX Boot Loader cryptographic Module (First-Stage Boot Loader)	RSA SigVer 4096	A3120	RSA digital signature verification for trusted update.
	For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [P-256, P-384]; ISO/IEC 14888-3, Section 6.4	SpaceX Cryptographic Module (BoringSSL) NXP JCOP4 EC Component For N7121 (Secure Element Chip)	ECDSA SigGen, sigVer over P-256 or P-384	A3452 C1429	ECDSA Signature operations for IKEv2 SA's ECDSA signature operations for SSH public key authentication.
FCS_COP.1/ Hash	[SHA-256, SHA-384] and message digest sizes [256, 384] bits	SpaceX Cryptographic Module (BoringSSL) SpaceX Uboot cryptographic Module SpaceX Cryptographic Module (BoringSSL)	SHA2-384 SHA2-256 SHA2-384	A3452 A3122 A3452	IPsec Phase 1 SA hashing Trusted Update hash comparison, firmware integrity verification ECDH-SHA2 key exchange in SSH

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #	TSF Supported
FCS_COP.1/ KeyedHash	[HMAC-SHA-384,] and cryptographic key sizes [384] and message digest sizes [384] bits	SpaceX Cryptographic Module (BoringSSL) SpaceX Linux Kernel cryptographic Module	HMAC-SHA2-384	A3452 A3121	Message authentication codes for IPsec SA's
FCS_RBG_EXT.1	CTR_DRBG (AES-256)	NXP JCOP4 DRBG Component For N7121 (Secure Element Chip)	CTR_DRBG with AES-256	C886	DRBG for all TOE functions.

End of Document